On the Existence of Irreducible Polynomials with Prescribed Coefficients over Finite Fields

by

Georgios Tzanakis, B.Math

A thesis submitted to
the Faculty of Graduate Studies and Research
in partial fulfillment of
the requirements for the degree of
Master of Science

School of Mathematics and Statistics
Ottawa-Carleton Institute for Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada

©Copyright
2010, Georgios Tzanakis
To the memory of my grandmother, Lela
Abstract

Let $q$ be a prime power and $F_q$ the finite field with $q$ elements. We examine the existence of irreducible polynomials with prescribed coefficients over $F_q$. We focus on a conjecture by Hansen and Mullen [25, Conjecture A] which states that for $n \geq 3$, there exist irreducible polynomials over $F_q$ with any one coefficient prescribed to any element of $F_q$ (this being nonzero when the constant coefficient is being prescribed) and was proven by Wan [42]. We introduce a variation of Wan’s method to give restrictions subject to which this result can be extended to more than one prescribed coefficient. It also follows from our generalization the existence of irreducible polynomials with sequences of consecutive zero coefficients.
Acknowledgements

First, I must acknowledge my defense committee and thank them for all of their comments and insights. The committee includes Lucy Campbell, Daniel Panario and Saban Alaca, from the School of Mathematics and Statistics at Carleton University, Evangelos Kranakis from the School of Computer Science at Carleton University, and Monica Nevins from the Department of Mathematics and Statistics at the University of Ottawa.

Thanks to the School of Mathematics and Statistics at Carleton University and my supervisor Daniel Panario for their generous funding. Thanks to the inspiring professors and researchers Theo Garefalakis, Lucia Moura, Monica Nevins, Daniel Panario, and Damien Roy. Thanks to the stuff, particularly Cate Palmer for working hard to make the life of the students easier.

Special thanks to Theo Garefalakis from the Department of Mathematics at University of Crete, for introducing me to mathematical research and to the topic of this thesis, in particular, as well as suggesting me to study at Carleton University under the supervision of Daniel Panario. Special thanks to my supervisor Daniel Panario for his efforts and precious help in my academic and non-academic life. Working under his supervision was a pleasure and a most valuable experience.

I must thank all the people who supported me during my studies in Canada, most importantly my parents Nikos and Maro Tzanakis, my sister Eleni Tzanakis and her family, and my uncle Dimos Mikedakis, whose love and care I could take for granted while I was so far away from home. Thanks to Ali Al-Bashabsheh for being the friend that I needed so much during my time here. Thanks to Petros, Nikos and Lefteris Gorgoraptis, for always being like brothers, no matter the distance between us. Thanks to all the people who got into my life and with whom we shared wonderful moments during my staying in Canada in the last two years, especially Tony Lai, Tim Winzler, Katrin Lambacher, Kristin Hübner, Lorena Lbacache, Inka Reichert, Karolina Thel, and Marta Ryżewska.
Contents

Abstract iii

Acknowledgements v

1 Introduction 1

2 Preliminaries 5

2.1 Finite fields ......................................................... 5
  2.1.1 Existence and uniqueness of finite fields ......................... 5
  2.1.2 Notations, definitions, and useful facts ........................... 8

2.2 Euler’s formula for multiplicative functions ........................... 9

2.3 The number of irreducible polynomials ................................ 12

2.4 Dirichlet characters and Dirichlet L-series ........................... 15

2.5 Bounds of character sums ............................................. 19

3 Previous Results 25

3.1 Dirichlet’s Theorem ................................................... 25

3.2 Hansen-Mullen Conjecture ............................................. 31

3.3 Consecutive zero coefficients ......................................... 31

3.4 Other results ........................................................ 32
  3.4.1 Irreducible polynomials with a few non-zero coefficients ........ 33
  3.4.2 Irreducible polynomials with a few prescribed coefficients .... 34

4 New Results 35

4.1 The main theorem .................................................... 35
4.2 Generalizing Hansen-Mullen Conjecture .......................................................... 40
4.3 Consecutive zero coefficients ........................................................................... 43

5 Conclusions ........................................................................................................ 47
5.1 Summary of results ........................................................................................... 47
5.2 Open questions for further work ...................................................................... 48
Chapter 1

Introduction

Finite fields (or Galois fields) are algebraic fields with a finite number of elements. The study of these algebraic structures can be originally traced back to the works of Gauss and Galois, but has become increasingly important in recent years, mainly due to their diverse applications in Coding Theory (many codes are constructed as subspaces of vector spaces over finite fields) and Cryptography (a number of cryptographic algorithms rely heavily on properties of finite fields).

One of the most important tools for investigating the algebraic structure of finite fields is the theory of polynomials over a finite field. Much attention has been given to the study of irreducible polynomials (the prime elements of the polynomial ring over a finite field), since the most usual way to represent a finite field is by using a polynomial basis, which is constructed from the root of an irreducible polynomial over a finite field.

Let $F$ be a finite field, $m, n$ integers with $1 \leq m \leq n$, $\alpha \in F$ and suppose there exists an irreducible polynomial $P$ of degree $n$ over $F$ with the coefficient of $x^m$ being $\alpha$. We say that we can prescribe the coefficient of $x^m$ of $P$ to $\alpha$. One aspect of the study of polynomials over finite fields which has been researched extensively is that of irreducible polynomials with prescribed coefficients. More precisely, it is a common research topic to question the existence or evaluate the number of irreducible polynomials with certain patterns of prescribed coefficients. This kind of polynomials may be of practical interest (for instance, Coppersmith’s algorithm [14] for discrete logarithm computations uses irreducible polynomials over finite fields with characteristic 2, with many consecutive zero coefficients) or of pure mathematical one (see for example the Hansen-Mullen Conjecture [25]). In this thesis we study the existence of irreducible polynomials with coefficients prescribed to any value or with many consecutive zero coefficients, using number theoretical tools adapted to the context of the ring of polynomials over finite fields, and ideas similar to the ones by Wan [42] and Garefalakis [21].
We try to make our work self-contained, assuming only some basic knowledge of rings and fields. In Chapter 2 we give all the preliminaries that are needed for the rest of the thesis. We start by briefly introducing finite fields and characterizing them completely. We adapt a proof of Euler’s formula for multiplicative functions found in [2] to the ring of polynomials over finite fields. We also present Dirichlet’s characters and their corresponding L-series in this context, as well as any related tool that is needed in the next chapters of the thesis. In the last section, we show some very important bounds for character sums (for instance Weil’s bound) which are the cornerstone of many of the most significant results in this area, as well as the new results presented in this thesis.

In Chapter 3 we give an overview of the previous results in the area, focusing on the ones that are based on Weil’s bound. We present Dirichlet’s theorem for primes in arithmetic progressions in the context of the ring of polynomials over a finite field and several generalizations, explaining how one derives from them some of the strongest results regarding irreducible polynomials with prescribed coefficients. We present the Hansen-Mullen Conjecture and discuss how Wan [42] settles it. Due to their importance in applications, we also discuss irreducible polynomials with many consecutive zero coefficients. We close the chapter by briefly presenting results that are obtained using completely different techniques, focusing on two types of polynomials: irreducible polynomials with a few prescribed coefficients, and irreducible polynomials with a few non-zero coefficients.

In Chapter 4 we present our new results. In the first section, we give our main theorem, which is based on ideas of Wan [42] and Garefalakis [21] and, in fact, gives generalizations of their results. In the next section, we use our main theorem to obtain a generalization of the Hansen-Mullen Conjecture; we give conditions under which any number of coefficients can be prescribed to any value, and give examples of some interesting cases. In the last section, we use our main theorem to obtain results about the existence of irreducible polynomials with sequences of consecutive zero coefficients.

In Chapter 5, we give a summary of our new results and pose some open questions that are in the spirit of this work and could be considered for future research.

Lastly, we would like to mention (and, in fact, stress) that in this thesis we do not consider primitive polynomials (minimal polynomials of generator elements of the multiplicative group of a finite field) or normal polynomials (irreducible polynomials whose roots generate a normal basis over a finite field, see [32, Definition 2.32]). These are very important classes of irreducible polynomials and prescribing their coefficients has been the focus of substantial recent research (see for example...
[10, 11, 12, 13, 16, 17, 18, 19]). However, being comprehensive on those polynomials is beyond the scope of our work, and we prefer to focus on irreducible polynomials only.
Chapter 2

Preliminaries

2.1 Finite fields

2.1.1 Existence and uniqueness of finite fields

In this section we provide a very brief introduction to the theory of finite fields, including their complete characterization. We assume some basic knowledge of rings and fields. For a complete and thorough presentation of the subject, the reader is referred to [32].

The following are well known facts from Algebra.

• If \( p \) is a prime, the ring \( \mathbb{Z}/p\mathbb{Z} \) is a field with \( p \) elements which we denote \( \mathbb{F}_p \).

• The ring \( \mathbb{F}_p[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \ a_i \in \mathbb{F}_p\} , n \in \mathbb{N} \) of polynomials over \( \mathbb{F}_p \) is an Euclidean domain.

• If \( R \) is a ring and \( I \) is an ideal of \( R \), then \( R/I \) is a field if and only if \( I \) is maximal.

Let \( f \in \mathbb{F}_p[x] \) and consider the ring

\[
\mathbb{F}_p[x]/f\mathbb{F}_p[x] = \{a + f\mathbb{F}_p[x], \ a \in \mathbb{F}_p[x]\}.
\]

**Proposition 2.1.1.** If \( f \in \mathbb{F}_p[x] \) is irreducible then the ring \( \mathbb{F}_p[x]/f\mathbb{F}_p[x] \) is a field.

**Proof.** Let \( f \in \mathbb{F}_p[x] \) be irreducible. From the above, we only need to show that the ideal \( f\mathbb{F}_p[x] \) is maximal. Suppose there exists an ideal \( I \) of \( \mathbb{F}_p[x] \) such that \( f\mathbb{F}_p[x] \subseteq I \subseteq \mathbb{F}_p[x] \). If \( I \neq f\mathbb{F}_p[x] \), then there exists a \( h \in I \setminus f\mathbb{F}_p[x] \) of least degree. Since \( \mathbb{F}_p[x] \) is an Euclidean domain, then there exist
$g, r \in \mathbb{F}_p[x]$ such that $h = fg + r$ with $\deg(r) < f$. Because $h \not\in f\mathbb{F}_p[x]$, we have $r \neq 0$ and $r \in I \setminus f\mathbb{F}_p[x]$, so $\deg(r) \geq \deg(h)$, from the definition of $h$. But $\deg(h) = \deg(fg + r) \geq \deg(f) > \deg(r)$, which is a contradiction. This completes the proof that $f\mathbb{F}_p[x]$ is a maximal ideal of $\mathbb{F}_p[x]$. \qed

Remark 2.1.2. Let $f \in \mathbb{F}_p[x]$ and

$$H = \{a \in \mathbb{F}_p[x] \text{ such that } \deg(a) < \deg(f)\}.$$  

We have that $H$ is a complete system of representatives of $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$, so the latter has exactly $p^{\deg(f)}$ elements. From now on, we identify the classes of $\mathbb{F}_p[x]/f\mathbb{F}_p[x]$ with their representatives and we only use representatives from $H$.

Given a prime $p$, a positive integer $n$ and an irreducible $f \in \mathbb{F}_p[x]$ of degree $n$, we constructed a finite field with $p^n$ elements. It is now natural to ask if for every prime $p$ and positive integer $n$ there exists an irreducible $f \in \mathbb{F}_p[x]$ of degree $n$ (and consequently a finite field with $p^n$ elements). The answer to this question is positive and is an immediate consequence of Theorem 2.3.4 (to be given later) for the case when $(p,n) \neq (2,2)$. For the case $(p,n) = (2,2)$, one can easily check that, for instance, $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$.

We have shown that for every prime $p$ and for every positive integer $n$ there exists a finite field with $p^n$ elements. We now prove that the converse is also true.

**Proposition 2.1.3.** Let $F$ a finite field of characteristic $p$. Then $F$ has $p^n$ elements for some positive integer $n$.

**Proof.** Since $F$ has characteristic $p$ (which is of course a prime), its prime subfield is isomorphic to $\mathbb{Z}_p$. Then $F$ is a vector space over $\mathbb{Z}_p$ and thus has a basis $\alpha_0, \ldots, \alpha_{n-1}$ over $\mathbb{Z}_p$ for some integer $n \geq 1$. Any element in $F$ is then of the form

$$a_0 \alpha_0 + a_1 \alpha_1 + \cdots + a_{n-1} \alpha_{n-1}, \text{ with } a_i \in \mathbb{Z}_p, \ i = 0, \ldots, n - 1,$$

and, clearly, there are $p^n$ such elements. \qed

**Conclusion.** The cardinality of any finite field is a prime power, and every prime power is the cardinality of some finite field.
We have shown the existence of finite fields. We now show that every finite field is unique up to isomorphism.

**Definition 2.1.4.** The extension field $K$ of a field $F$ is called a splitting field of the polynomial $f \in F[x]$, if $f$ factors completely into linear factors in $K$ and it does not factor in any subfield of $K$ containing $F$.

From [15, Section 13.4; Theorem 25 and Corollary 28] we have the following.

**Theorem 2.1.5** (Existence and uniqueness of splitting fields). Let $F$ be a field and $f \in F[x]$. Then there exists a splitting field $E$ of $f$ over $F$ and any two splitting fields of $f$ over $F$ are isomorphic under an isomorphism which fixes $F$ and maps roots of $f$ into each other.

**Definition 2.1.6.** A polynomial is separable over a field $K$, if all of its irreducible factors have distinct roots in an algebraic closure of $K$.

The next lemma follows from [15, Section 13.5; Proposition 33].

**Lemma 2.1.7.** Let $F$ be a field and $f \in F[x]$. Then $f$ is separable over $F$ if and only if $\gcd(f, f') = 1$.

**Example 2.1.8.** Let $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$. Since $f'(x) = p^n x^{p^n-1} - 1 = -1$ over $\mathbb{F}_p$, then $(f, f') = 1$ and, from the previous lemma, $f$ is separable over $\mathbb{F}_p$.

**Theorem 2.1.9.** Let $p$ be a prime number, $n$ a positive integer and $F$ a finite field of $p^n$ elements. Then $F$ is isomorphic to the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$.

**Proof.** Let $f(x) = x^{p^n} - x$. This, as shown in example 2.1.8, is separable over $\mathbb{F}_p$ and thus has exactly $p^n$ distinct roots.

Let $A$ be the set of roots of $f$ over $\mathbb{F}_p$. One can check that $A$ is a field, thus a subfield of the splitting field of $f$ over $\mathbb{F}_p$. Then, from the minimality of the splitting field, $A$ has to be the splitting field of $f$ over $\mathbb{F}_p$. We have shown that the splitting field of $f$ over $\mathbb{F}_p$ has $p^n$ elements.

Now, let $F$ be a finite field with $p^n$ elements. Since $F^*$ has order $p^n - 1$, then for every $\alpha \in F^*$ we have $\alpha^{p^n-1} = 1$, and so $\alpha^{p^n} = \alpha$. Hence, every element of $F$ is a root of $f$ and thus $F \subseteq A$. But since $|A| = p^n$, then $F = A$. The uniqueness of the finite field with $p^n$ elements then follows from the uniqueness of splitting fields.
2.1.2 Notations, definitions, and useful facts

In this section we give the fundamental background for this thesis, as well as definitions and notations. For the rest of this thesis we consider a fixed prime power \( q \) and we denote by \( \mathbb{F}_q \) the finite field with \( q \) elements.

We start with some definitions regarding polynomials over finite fields.

**Definition 2.1.10.** Let \( f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{F}_q[x] \). If \( a_n \neq 0 \), we set \( \text{sgn}(f) = a_n \) and call this element of \( \mathbb{F}_q \) the **sign** of \( f \). We define the **absolute value** \( |f| \) of \( f \) to be \( q^n \). We call \( a_{n-1} \) and \( a_{n-2} \) the **trace** and **subtrace** of \( f \) respectively. Let \( m, n \) positive integers with \( m \leq n \). We call \( a_0, a_1, \ldots, a_m \) the \( m \) **least significant** and \( a_n, \ldots, a_{n-m+1} \) the \( m \) **most significant** coefficients of \( f \), respectively.

**Definition 2.1.11.** We define \( \Phi(f) \) to be the number of elements in the group \((\mathbb{F}_q[x]/f\mathbb{F}_q[x])^*\). This is the generalization of Euler’s function in \( \mathbb{F}_q[x] \), as it is the number of non-zero polynomials of degree less than \( \deg(f) \) and relatively prime to \( f \). The next proposition is an immediate consequence of [40, Proposition 1.7].

**Proposition 2.1.12.** We have \( \Phi(x^n) = q^{n-1}(q - 1) \).

Another class of polynomials which are important for our work is the **primary polynomials**.

**Definition 2.1.13.** A polynomial in \( \mathbb{F}_q[x] \) is called **primary** if it is a power of an irreducible polynomial in \( \mathbb{F}_q[x] \).

Related to primary polynomials, is the **Von Mangolt \( \Lambda \) function**, another tool of number theory in the context of polynomials over finite fields.

**Definition 2.1.14.** The **Von Mangolt function** \( \Lambda \) over \( \mathbb{F}_q[x] \) is defined as

\[
\Lambda(g) = \begin{cases} 
\deg(P) & \text{if } g = P^e \text{ for some monic irreducible } P \in \mathbb{F}_q[x] \text{ and integer } e, \\
0 & \text{otherwise.}
\end{cases}
\]

**Definition 2.1.15.** Let \( f(x) = \sum_{i=0}^n a_i x^i \). We call \( \sum_{i=0}^n a_{n-i} x^i \) the **reciprocal** of \( f \).
In this thesis, we are concerned about polynomials with prescribed coefficients; once the existence of an irreducible polynomial of a particular form is granted, the following lemma yields the existence of another irreducible polynomial of a particular form.

**Lemma 2.1.16.** A polynomial over a finite field is irreducible if and only if its reciprocal is irreducible.

*Proof.* Let $f \in \mathbb{F}_q[x]$ with degree $n$ and $g$ be the reciprocal of $f$. Suppose by contradiction that $f$ is irreducible but $g$ is not and let $\theta$ be a root of $f$ in some extension of $\mathbb{F}_q$. Observe that $g(x) = x^n f(1/x)$.

Then $1/\theta$ is a root of $g$ and $1/\theta \in \mathbb{F}_q(1/\theta) = \mathbb{F}_q(\theta) = \mathbb{F}_{q^n}$. Since $1/\theta$ is a root of $g$, then it is also the root of an irreducible polynomial $h$ over $\mathbb{F}_q$, with $h|g$. It cannot be $\deg(h) < n$ since in that case we would have $\mathbb{F}_{q^n} = \mathbb{F}(1/\theta) = \mathbb{F}_{q^{\deg(h)}}$ which is clearly not true. Then $\deg(h) = n$ and thus $g$ has to be irreducible, which contradicts our hypothesis. The proof of the converse is exactly the same.

We close this section by gathering together the notations that we use in this thesis.

- $\mathbb{F}_q$ denotes the finite field with $q$ elements;
- $A := \mathbb{F}_q[x]$, where $\mathbb{F}_q[x]$ is the ring of polynomials over the finite field with $q$ elements;
- $\mathbb{M}$ denotes the set of monic polynomials in $A$;
- $\mathbb{I}$ denotes the set of monic irreducible polynomials in $A$;
- $\mathbb{M}_n$, and $\mathbb{I}_n$ denote the sets of polynomials with degree $n$ in $\mathbb{M}$ and $\mathbb{I}$, respectively;
- $I_n$ denotes the cardinality of $\mathbb{I}_n$;
- $\mathbb{H}_n$ denotes the set of primary monic polynomials in $A$ with degree $n$, for $n \geq 1$; we set $\mathbb{H}_0 = \{1\}$.

### 2.2 Euler’s formula for multiplicative functions

In this section we prove Euler’s formula for multiplicative functions. This is a very fundamental tool and is used to obtain some of the most important results of the next chapter. Our proof is based on [2, Theorem 11.6] for Euler’s formula in the context of number theory.

Let $(a_n)_{n \in \mathbb{N}}$ be a sequence of complex numbers. We say that an infinite product of the form $\prod_{n \in \mathbb{N}} (1 + a_n)$ converges absolutely if the product $\prod_{n \in \mathbb{N}} (1 + |a_n|)$ converges. From a well-known theorem of complex analysis, we know that $\prod_{n \in \mathbb{N}} (1 + a_n)$ converges if and only if $\sum_{n \in \mathbb{N}} a_n$ converges absolutely. From the fact that the elements of $\mathbb{M}$ are enumerable, we have the following theorem.
Theorem 2.2.1. Let $h: \mathbb{M} \rightarrow \mathbb{C}$. Then the product $\prod_{f \in \mathbb{M}} (1 + h(f))$ converges absolutely if and only if the series $\sum_{f \in \mathbb{M}}|h(f)|$ converges.

We now introduce the notion of multiplicative functions.

Definition 2.2.2. A non-zero function $h: \mathbb{M} \rightarrow \mathbb{C}$ is called multiplicative if $h(f_1 f_2) = h(f_1) h(f_2)$ for every coprime $f_1$ and $f_2$, and completely multiplicative if $h(f_1 f_2) = h(f_1) h(f_2)$ for every $f_1$ and $f_2$.

We have the following theorem for completely multiplicative functions.

Theorem 2.2.3. If $h: \mathbb{M} \rightarrow \mathbb{C}$ is multiplicative and $h(1) = 1$, then it is completely multiplicative if and only if $h(P^k) = h(P)^k$ for every $P \in \mathbb{I}$ and integer $k \geq 1$.

We are now ready to present Euler’s formula for multiplicative functions.

Theorem 2.2.4 (Euler’s formula for multiplicative functions). Let $h: \mathbb{M} \rightarrow \mathbb{C}$ be multiplicative such that $\sum_{f \in \mathbb{M}} |h(f)|$ converges. Then

$$\sum_{f \in \mathbb{M}} h(f) = \prod_{P \in \mathbb{I}} (1 + h(P) + h(P^2) + \cdots).$$

(2.1)

If $h$ is also completely multiplicative, then

$$\sum_{f \in \mathbb{M}} h(f) = \prod_{P \in \mathbb{I}} (1 - h(P))^{-1}.$$  

Proof. Let $P \in \mathbb{M}$. Clearly $\{P^i, i \in \mathbb{N}\} \subset \mathbb{M}$, so, since $\sum_{f \in \mathbb{M}} h(f)$ converges absolutely, then $h(P) + h(P^2) + \cdots$ also converges absolutely.

Consider the finite product

$$P(n) = \prod_{\substack{P \in \mathbb{I} \\text{deg}(P) \leq n}} (1 + h(P) + h(P^2) + \cdots).$$

Since this is the product of a finite number of absolutely convergent series, we can multiply the series and rearrange the terms in any fashion without altering the sum. A typical term is of the form

$$h(P_1^{a_1}) h(P_2^{a_2}) \cdots h(P_r^{a_r}) = h(P_1^{a_1} P_2^{a_2} \cdots P_r^{a_r}),$$

\[ \sum_{f \in \mathbb{M}} h(f) = \prod_{P \in \mathbb{I}} (1 + h(P) + h(P^2) + \cdots). \]
since $h$ is multiplicative. Hence,

$$P(n) = \sum_{f \in A} h(f),$$

where $A$ consists of those $f \in \mathbb{M}$ formed by irreducible factors of degree at most $n$. Therefore,

$$\sum_{f \in \mathbb{M}} h(f) - P(n) = \sum_{f \in B} h(f),$$

where $B$ is the set of those $f \in \mathbb{M}$ with at least one irreducible factor $P$ having $\deg(P) > n$. Then,

$$\left| \sum_{f \in \mathbb{M}} h(f) - P(n) \right| \leq \sum_{f \in B} |h(f)| \leq \sum_{f \in \mathbb{M}, \deg(f) > n} |h(f)|.$$

As $n \to +\infty$, the last sum on the right tends to zero, since $\sum |h(f)|$ is convergent. Hence

$$\lim_{n \to +\infty} P(n) = \sum_{f \in \mathbb{M}} h(f). \quad (2.2)$$

Now,

$$\sum_{P \in I, |P| \leq n} |h(P) + h(P^2) + \cdots| \leq \sum_{P \in I, |P| \leq n} (|h(P)| + |h(P^2)| + \cdots) \leq \sum_{f \in \mathbb{M}} |h(f)|,$$

where, from our assumption, the sum in the right-most side converges. As we have already mentioned, an infinite product $\prod (1 + a_n)$ converges absolutely if and only if $\sum a_n$ converges absolutely. In our case, since all partial sums like the one in the left-most side are bounded, the series of positive terms $\sum_{P \in I} |h(P) + h(P^2) + \cdots|$ converges and, consequently, $\prod_{P \in I} (1 + h(P) + h(P^2) + \cdots)$ is absolutely convergent. But this infinite product is equal to $\lim_{n \to +\infty} P(n)$, and this, combined with (2.2) proves our first claim.

Now, when $h$ is completely multiplicative, we have from Theorem 2.2.3 that for every $P \in \mathbb{I}$

$$1 + h(P) + h(P^2) + \cdots = 1 + h(P) + h(P)^2 + \cdots.$$

The sum on the right of the above equation converges absolutely, so it must be $|h(P)| < 1$ and therefore

$$1 + h(P) + h(P^2) + \cdots = (1 - h(P))^{-1}.$$
That proves that for a completely multiplicative $h$, we have

$$
\sum_{f \in \mathcal{M}} h(f) = \prod_{P \in \mathbb{P}} (1 - h(P))^{-1}.
$$

\[ \square \]

### 2.3 The number of irreducible polynomials of a certain degree

In this section we give bounds for the number of irreducible polynomials of a fixed degree. We start with a lemma that comes in handy, as in the rest of this thesis we often have to compute the logarithmic derivative of expressions of some certain form.

**Lemma 2.3.1.** Let $\alpha \in \mathbb{C}, k \in \mathbb{N}$ and $|u|^k < |\alpha|^{-1}$. Then

$$u \frac{d}{du} \log(1 - \alpha u^k) = -k \sum_{i=1}^{\infty} \alpha^i u^{ki}. \quad (2.3)$$

**Proof.** We have

$$u \frac{d}{du} \log(1 - \alpha u^k) = u \frac{-\alpha k u^{k-1}}{1 - \alpha u^k} = -\alpha ku^k \frac{1}{1 - \alpha u^k},$$

and since $|u|^k < |\alpha|^{-1}$, the last expression can be written as

$$-\alpha ku^k \sum_{i=0}^{\infty} \alpha^i u^{ki} = -k \sum_{i=1}^{\infty} \alpha^i u^{ki}.$$

\[ \square \]

Let $s \in \mathbb{C}$. Then

$$\sum_{g \in \mathcal{M}} |g|^{-s} = \sum_{m=0}^{\infty} \sum_{g \in \mathcal{M}_m} \frac{1}{|g|^s}$$

Observing that $|\mathcal{M}_m| = q^m$, we have that the last sum is equal to

$$\sum_{m=0}^{\infty} q^m q^{-sm} = \sum_{m=0}^{\infty} q^{m(1-s)}.$$

This last power series converges if and only if $\Re(s) > 1$, so the same applies for $\sum_{g \in \mathcal{M}} |g|^{-s}$. 

Remark 2.3.2. The function \( \zeta_A(s) = \sum_{g \in M} |g|^{-s}, s \in \mathbb{C}, \Re(s) > 1 \) is the analogue of the \textit{Zeta function} for the ring of polynomials over finite fields.

**Proposition 2.3.3** (Euler’s formula for the zeta function). We have

\[
\zeta_A(s) = \prod_{P \in I} \left(1 - \frac{1}{|P|^s}\right)^{-1}, \Re(s) > 1.
\]

\textit{Proof.} We apply Theorem 2.2.4 for the completely multiplicative function \( f : A \rightarrow \mathbb{C} \) with \( f(g) = |g|^{-s}, \Re(s) > 1 \).

Recall that \( I_n \) denotes the number of irreducible polynomials with degree \( n \). From Proposition 2.3.3 we have

\[
\zeta_A(s) = \prod_{d=1}^{\infty} \left(1 - q^{-ds}\right)^{-I_d}. \tag{2.4}
\]

Since there are exactly \( q^n \) monic polynomials of degree \( n \) over \( \mathbb{F}_q \), then

\[
\sum_{\deg(g) \leq d} |g|^{-s} = 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \cdots + \frac{q^d}{q^{ds}},
\]

and hence, for \( \Re(s) > 1 \), we have

\[
\zeta_A(s) = \lim_{d \to \infty} \sum_{\deg(g) \leq d} |g|^{-s} = \lim_{d \to \infty} \left(1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \cdots + \frac{q^d}{q^{ds}}\right) = \sum_{d=0}^{\infty} q^d(1-s)
\]

Substituting \( q^{-s} \) with \( u \) in (2.4) and the above equation, we get

\[
\frac{1}{1 - qu} = \prod_{d=1}^{\infty} \left(1 - u^d\right)^{-I_d}
\]

Considering \( \Re(s) > 1 \) and taking logarithmic derivatives multiplied by \( u \) on both sides (see also Lemma 2.3.1), we get

\[
\frac{qu}{1 - qu} = \sum_{d=1}^{\infty} I_d \frac{du^d}{1 - u^d}. \tag{2.5}
\]
Now, the left side of the above equation can be written as

\[
\frac{qu}{1-qu} = \sum_{n=0}^{\infty} (qu)^{n+1} = \sum_{n=1}^{\infty} q^n u^n. \tag{2.6}
\]

We also have

\[
\frac{ud}{1-ud} = u \sum_{k=0}^{\infty} ud^k = \sum_{k=0}^{\infty} u^{d(k+1)} = \sum_{k=1}^{\infty} ud^k,
\]

so

\[
\sum_{d=1}^{\infty} I_d \frac{du^d}{1-u^d} = \sum_{d=1}^{\infty} dI_d \sum_{k=1}^{\infty} u^d = \sum_{d=1}^{\infty} \sum_{k=1}^{\infty} dI_d u^d = \sum_{n=1}^{\infty} \left( \sum_{d|n} dI_d \right) u^n. \tag{2.7}
\]

From (2.5), (2.6), and (2.7), we deduce that

\[
\sum_{d|n} dI_d = q^n, \tag{2.8}
\]

and Möbius inversion formula then yields

\[
I_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}. \tag{2.9}
\]

We have the following key result regarding the number of irreducible polynomials of a certain degree over a finite field.

**Theorem 2.3.4.** For \( n \geq 2 \) we have

\[
\frac{q^n}{n} - \frac{2q^n}{n} \leq I_n \leq \frac{q^n}{n} - \frac{q}{n}.
\]

**Proof.** Let \( p \) be the smallest prime divisor of \( n \). Then, since \( \mu(d) = 1, -1, \) or \( 0 \), we have

\[
nI_n = \sum_{d|n} \mu(d) q^{\frac{n}{d}} = q^n - q^\frac{n}{d} \leq q^n - q^\frac{n}{p} + \sum_{d>n, d>p} q^\frac{n}{d} \leq q^n - q^\frac{n}{p} + \sum_{i=1}^{\frac{n}{p}-1} q^i
\]

\[
= q^n - q^\frac{n}{p} + q^{\frac{n}{p}-1} - 1 \leq q^n - q.
\]

and we have the upper bound. For the lower bound, we have
2.4 Dirichlet characters and Dirichlet $L$-series

Definition 2.4.1. Let $G$ be a finite abelian group (written multiplicatively). A character $\chi$ of $G$ is a homomorphism from $G$ into the multiplicative group $\mathbb{C}^*$ of complex numbers of absolute value 1. We denote $\hat{G}$ the set of all characters of $G$. The character $\chi_0$ that maps every $g \in G$ to 1 is called the trivial character. With each character $\chi$ of $G$ there is associated the conjugate character $\overline{\chi}$ defined by $\overline{\chi}(g) = \chi(g)$ for all $g \in G$.

We define the product of two characters $\chi$, $\psi$ of $G$ by setting $\chi \psi(g) = \chi(g)\psi(g)$ for all $g \in G$. Clearly the set $\hat{G}$ of characters of $G$ is a multiplicative group under this product, the trivial character being the neutral element and the conjugate of a character being its inverse.

Let $\delta$ be the Kronecker’s delta function, that is, $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ if $i \neq j$.

Proposition 2.4.2. The following are well known facts of group theory (see [32, Chapter 5]).

1. If $\chi$ is a character of $G$, then $|\chi(a)| = 1$ for every $a \in G$;
2. $|\hat{G}| = |G|$;
3. $\sum_{g \in G} \chi(g)\overline{\psi(g)} = |G|\delta_{\chi,\psi}$ for any $\chi, \psi \in \hat{G}$;
4. $\sum_{\chi \in \hat{G}} \chi(g)\overline{\chi(h)} = |G|\delta_{g,h}$ for any $g, h \in G$.

Consider a character $\chi$ of the multiplicative group $(A/fA)^*$. A Dirichlet character modulo $f$ is an extension of $\chi$ to $A$ by zero. More precisely, we have the following definition.

Definition 2.4.3. Let $f \in A$ of positive degree. A Dirichlet character modulo $f$ is a map $\chi$ from $A$ to $\mathbb{C}$ such that for all $a, b \in A$
1. \( \chi(a + bf) = \chi(a) \),

2. \( \chi(a)\chi(b) = \chi(ab) \),

3. \( \chi(a) = 0 \iff (a, f) \neq 1 \).

It follows that \( |\chi(a)| = 1 \) when \( \chi(a) \neq 0 \). The Dirichlet character \( \chi_0 \) modulo \( f \) which maps all \( a \in \mathbb{A} \) with \( (a, f) = 1 \) to 1 is called the trivial Dirichlet character. We denote the set of all Dirichlet characters modulo \( f \) as \( X_f \). With each Dirichlet character \( \chi \) modulo \( f \) there is associated the conjugate character \( \overline{\chi} \) defined by \( \overline{\chi}(a) = \overline{\chi(a)} \) for all \( a \in \mathbb{A} \).

We define the product of two Dirichlet characters by setting \( \chi \psi(a) = \chi(a)\psi(a) \) for all \( a \in \mathbb{A} \). This makes \( X_f \) into a group with the trivial Dirichlet character being the neutral element and the conjugate of a Dirichlet character being its inverse.

**Theorem 2.4.4.** \( X_f \) is isomorphic to \((\widehat{\mathbb{A}/f\mathbb{A}})^*\).

**Proof.** Denote \( \overline{a} \) the class of \( a \in \mathbb{A} \) in \((\mathbb{A}/f\mathbb{A})^*\). Consider the map

\[
\theta : X_f \rightarrow (\widehat{\mathbb{A}/f\mathbb{A}})^*
\]

\[
\chi \mapsto \widehat{\chi}
\]

where \( \widehat{\chi}(\overline{a}) = \chi(a) \) for every \( \overline{a} \in (\mathbb{A}/f\mathbb{A})^* \). We show that this is a group isomorphism.

First, \( \theta \) is a well defined homomorphism: if \( \overline{a}, \overline{b} \in (\mathbb{A}/f\mathbb{A})^* \) with \( \overline{a} = \overline{b} \), then \( a = b + gf \) for some \( g \in \mathbb{A} \) and so \( \widehat{\chi}(\overline{a}) = \widehat{\chi}(b + gf) = \chi(b + gf) = \chi(b) = \widehat{\chi}(\overline{b}) \). It is immediate to check that \( \widehat{\chi} \) is also a homomorphism. So \( \theta \) is indeed a character of \((\mathbb{A}/f\mathbb{A})^*\).

Suppose that \( \theta(\chi) = 1 \), that is, \( \widehat{\chi}(\overline{a}) = 1 \) for all \( a \) with \( (a, f) = 1 \). In other words, \( \chi \) is the trivial character and \( \ker(\theta) = \{\chi_0\} \). Thus \( \theta = 1 - 1 \).

Let \( \psi \in (\widehat{\mathbb{A}/f\mathbb{A}})^* \). Define \( \chi \) to be a function from \((\mathbb{A}/f\mathbb{A})^* \) to \( \mathbb{C}^* \) such that \( \chi(a) = \psi(\overline{a}) \) when \( (a, f) = 1 \) and \( \chi(a) = 0 \) otherwise. It is clear that \( \chi \in (\widehat{\mathbb{A}/f\mathbb{A}})^* \) and \( \theta(\chi) = \psi \). Thus \( \theta \) is surjective.

Finally, for \( \chi, \psi \in X_f \) we have \( \theta(\chi \psi) = \widehat{\chi \psi} = \widehat{\chi} \widehat{\psi} = \theta(\chi)\theta(\psi) \), thus \( \theta \) is a homomorphism and, from the above, an isomorphism.

\( \square \)

Using the isomorphism of this theorem we can obtain some useful corollaries.
Corollary 2.4.5. There are $\Phi(f)$ Dirichlet characters modulo $f$.

Proof. We have $|X_f| = |(\mathbb{A}/f\mathbb{A})^*| = |(\mathbb{A}/f\mathbb{A})^*| = \Phi(f)$, the first equality coming from Theorem 2.4.4 and the second one from part 2 of Proposition 2.4.2.

Corollary 2.4.6. We have the following orthogonality relations for Dirichlet characters

1. $\sum_h \chi(h)\overline{\psi(h)} = \Phi(f)\delta_{\chi,\psi}$ for any $\chi,\psi \in X_f$ and $\sum_h$ extends over any set of representatives of $\mathbb{A}/f\mathbb{A}$;

2. $\sum_{\chi \in X_f} \chi(a)\overline{\chi(b)} = \Phi(f)\delta_{a,b}$ for any $a, b \in \mathbb{A}$ coprime to $f$.

Proof. The proof is an immediate consequence of the orthogonality relations 3 and 4 in Proposition 2.4.2 and the homomorphism of Theorem 2.4.4.

Corollary 2.4.7. We have

1. $\sum_{h \in \mathbb{A}/f\mathbb{A}} \chi(h) = 0$ for any $\chi \in X_f$, $\chi \neq \chi_0$;

2. $\sum_{\chi \in X_f} \chi(h) = 0$ for any $h \in \mathbb{A}$, $h \neq 1$.

Proof. Part 1 comes from part 1 of Corollary 2.4.6 by setting $\psi = \chi_0$ and $\chi \neq \psi$, and part 2 comes from part 2 of Corollary 2.4.6 by setting $b = 1$ and $a \neq 1$.

For the new results that we present in Chapter 4, we prove a lemma regarding the product of Dirichlet characters.

Lemma 2.4.8. Let $\chi_1, \ldots, \chi_r$ be Dirichlet characters modulo $f_1, f_2, \ldots, f_r \in \mathbb{A}$, respectively. Then the map $\mathcal{X} : \mathbb{A} \to \mathbb{C}^*$ such that $\mathcal{X}(h) = \prod_{i=1}^r \chi_i(h)$ is a Dirichlet character modulo $\prod_{i=1}^r f_i$.

Proof. The fact that $\mathcal{X}$ is well-defined and multiplicative is an immediate consequence from the fact that $\chi_1, \ldots, \chi_r$ are well-defined homomorphisms. Finally, we have

$$\mathcal{X}(h) = 0 \Leftrightarrow \chi_i(h) = 0, \text{ some } i \in \{1, \ldots, r\}$$

$$\Leftrightarrow (h, f_i) \neq 1, \text{ some } i \in \{1, \ldots, r\}$$

$$\Leftrightarrow (h, \prod_{i=1}^r f_i) \neq 1.$$ 

From the above, $\mathcal{X}$ is a Dirichlet character modulo $\prod_{i=1}^r f_i$. 

CHAPTER 2. PRELIMINARIES

Considering the first part of Proposition 2.4.2 we have

$$\sum_{g \in M} \frac{|\chi(g)|}{|g|^s} \leq \sum_{g \in M} \frac{1}{|g|^s} = \zeta_A(s),$$

so, since \(\zeta_A(s)\) converges for \(\Re(s) > 1\), then \(\sum_{g \in M} \frac{|\chi(g)|}{|g|^s}\) also converges for \(\Re(s) > 1\). Having introduced the Dirichlet characters and discussed the convergence of \(\sum_{g \in M} \frac{|\chi(g)|}{|g|^s}\), we now define Dirichlet L-series corresponding to a Dirichlet character.

**Definition 2.4.9.** Let \(\chi\) be a Dirichlet character modulo \(f\). The Dirichlet L-series corresponding to \(\chi\) is defined as

$$L(s, \chi) = \sum_{g \in M} \frac{\chi(g)}{|g|^s}, \quad s \in \mathbb{C}, \ \Re(s) > 1. \quad (2.10)$$

Using Euler’s formula for multiplicative functions, we obtain an expression for \(L(s, \chi)\).

**Proposition 2.4.10.** For every Dirichlet character modulo \(f\) we have

$$L(s, \chi) = \prod_{P \in \mathbb{I}} \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}.$$  

*Proof.* We observe that \(h(P) = \chi(P)/|P|^s\) is a completely multiplicative function (see Definition 2.2.2). The proof is then an immediate consequence of Euler’s formula for multiplicative functions (Theorem 2.2.4).

Dirichlet series in the context of polynomials over finite fields, is the analogue of the Dirichlet series for integers. However they have a very convenient property that the latter do not have.

**Proposition 2.4.11.** If \(\chi\) is a non-trivial Dirichlet character modulo \(f\), then \(L(s, \chi)\) is a polynomial of \(q^{-s}\) over \(\mathbb{C}\) of degree at most \(\deg(f) - 1\).

*Proof.* We have that

$$L(s, \chi) = \sum_{g \in M} \frac{\chi(g)}{|g|^s} = \sum_{n=0}^{\infty} A(n, \chi)q^{-ns}$$

where

$$A(n, \chi) = \sum_{g \in M_n} \chi(g).$$

It is sufficient to show that \(A(n, \chi) = 0\) for all \(n \geq \deg(f)\). So, let \(n \geq \deg(f)\). Since \(\deg(g) = n\), we can write \(g\) in the form \(g = hf + r\), where \(\deg(r) \leq \deg(f)\) and \(h \in \mathbb{A}\) of degree \(n - \deg(f) \geq 0\), its
leading coefficient being $\text{sgn}(f)^{-1}$. On the other hand, every polynomial of degree $n \geq \text{deg}(f)$ can be written in this form in a unique way. We observe that $h$ can be chosen in $q^{n-\text{deg}(f)}$ ways. Thus,

\[
A(n, \chi) = \sum_r \sum_h \chi(hf + r) = \sum_r \sum_h \chi(r) = q^{n-\text{deg}(f)} \sum_r \chi(r) = 0,
\]

where the sums $\sum_r$ and $\sum_h$ run over all $r$ and $h$ as described above, and the last equality comes from the first part of Corollary 2.4.7.

For convenience, we are going to denote $L^*(u, \chi)$ the Dirichlet series $L(s, \chi)$, where $u = q^{-s}$.

### 2.5 Bounds of character sums

In this section we present some important bounds for character sums; these are the cornerstones of all the results presented in this thesis.

**Lemma 2.5.1.** Let $\chi$ be a non-trivial Dirichlet character modulo $f$. For $\Re(s) > 1$ and $u = q^{-s}$ we have

\[
u \frac{d}{du} \log(L^*(u, \chi)) = \sum_{n=0}^{\infty} c_n(\chi)u^n,
\]

where

\[
c_n(\chi) = -\sum_{k=1}^{l-1} \alpha_k(\chi)^n = \sum_{g \in M_\alpha} \Lambda(g)\chi(g),
\]

$l - 1$ is the degree of the polynomial $L^*(u, \chi)$ (see Proposition 2.4.11), and $\alpha_k(\chi)$, $k = 1, \ldots, l - 1$ are the inverses of its roots.

**Proof.** The constant term of $L^*(u, \chi)$ is

\[
\sum_{g \in M_0} \chi(g) = \chi(1) = 1,
\]

thus, from Proposition 2.4.11 we can write

\[
L^*(u, \chi) = \prod_{i=1}^{l-1} (1 - \alpha_i(\chi)u),
\]
where $l \leq \deg f$. From Lemma 2.3.1 for $k = 1$ we have

$$u \frac{d}{du} \log(L^*(u, \chi)) = u \frac{d}{du} \log \left( \prod_{k=1}^{l-1} (1 - \alpha_k(\chi)u) \right) = \sum_{k=1}^{l-1} u \frac{d}{du} \log(1 - \alpha_k(\chi)u)$$

$$= \sum_{k=1}^{l-1} \sum_{n=1}^{\infty} \alpha_k(\chi)^n u^n = \sum_{n=1}^{\infty} \left( -\sum_{k=1}^{l-1} \alpha_k(\chi)^n \right) u^n$$

so we have our first equation:

$$c_n(\chi) = -\sum_{k=1}^{l-1} \alpha_k(\chi)^n.$$ 

Now, from Proposition 2.4.10 we have

$$L(s, \chi) = \prod_{P \in \mathbb{P}} (1 - \chi(P)|P|^{-s})^{-1} = \prod_{d=1}^{\infty} \prod_{P \in \mathbb{P}_d} (1 - \chi(P)q^{-ds})^{-1}.$$ 

Thus, we have

$$L^*(u, \chi) = \prod_{d=1}^{\infty} \prod_{P \in \mathbb{P}_d} (1 - \chi(P)u^d)^{-1}$$

and

$$u \frac{d}{du} \log(L^*(u, \chi)) = u \frac{d}{du} \log \left( \prod_{d=1}^{\infty} \prod_{P \in \mathbb{P}_d} (1 - \chi(P)u^d)^{-1} \right)$$

$$= \sum_{d=1}^{\infty} \sum_{P \in \mathbb{P}_d} -u \frac{d}{du} \log(1 - \chi(P)u^d).$$

From Lemma 2.3.1, the last double sum is equal to

$$\sum_{d=1}^{\infty} \sum_{P \in \mathbb{P}_d} d \sum_{k=1}^{\infty} \chi(P)^k u^{dk} = \sum_{n=1}^{\infty} \left( \sum_{d|n} \sum_{P \in \mathbb{P}_d} \chi(P)^d \right) u^n.$$ 

Thus,

$$c_n(\chi) = \sum_{d|n} \sum_{P \in \mathbb{P}_d} d \chi(P)^d = \sum_{k|n} \sum_{P \in \mathbb{P}_{n/k}} \deg(P) \chi(P)^k = \sum_{k|n} \sum_{P \in \mathbb{P}_{n/k}} \deg(P) \chi(P^k)$$

$$= \sum_{g \in \mathbb{M}_n} \Lambda(g) \chi(g).$$
Remark 2.5.2. It follows from the analogue of the Riemann Hypothesis for function fields over a finite field that all $\alpha_k(\chi)$ as defined above have absolute value 1 or $\sqrt{q}$. This is the deepest part of the proof due to Weil (see [43]) which is beyond the scope of this thesis. This important fact yields a bound for $|c_n|$.

Corollary 2.5.3 (Weil’s Bound). Let $\chi$ be a non-trivial Dirichlet character modulo $f$ and $c_n$ as defined above. Then

$$|c_n(\chi)| \leq (\deg(f) - 1)q^{\frac{n}{2}}.$$  

Moreover, $c_n(\chi_0) = q^n$.

Proof. Consider the notations as in Lemma 2.5.1. From (2.8), we have

$$c_n(\chi_0) = \sum_{d|n} \sum_{P \in I_d} d = \sum_{d|n} d|I_d| = q^n.$$  

Now, let $\chi \neq \chi_0$. From Remark 2.5.2 we have $|\alpha_k(\chi)| \leq q^\frac{1}{2}$, so

$$|c_n(\chi)| = \left| -\sum_{k=1}^{l-1} \alpha_k(\chi)^n \right| \leq \sum_{k=1}^{l-1} |\alpha_k(\chi)|^n \leq \sum_{k=1}^{l-1} q^{\frac{n}{2}}$$

$$= (l - 1)q^{\frac{n}{2}} \leq (\deg(f) - 1)q^{\frac{n}{2}}.$$

This bound for $c_n$ is an important result and a very powerful tool. Having this bound we can now prove another key result, which is again a bound of another character sum. Recall that $I_n = |\mathbb{I}_n|$ as defined in Section 2.1.2.

Lemma 2.5.4. Let $c'_n(\chi) = \sum_{P \in \mathbb{I}_n} \chi(P)$. Then

$$|c'_n(\chi)| \leq \begin{cases} 
I_n & \text{when } \chi = \chi_0, \\
\frac{\deg(f)}{n}q^{\frac{n}{2}} & \text{when } \chi \neq \chi_0.
\end{cases}$$

Proof. In the case $\chi = \chi_0$ we have

$$\sum_{P \in \mathbb{I}_n} \chi_0(P) \leq \sum_{P \in \mathbb{I}_n} |\chi_0(P)| = \sum_{P \in \mathbb{I}_n} 1 = I_n.$$
Now let $\chi$ be a non-trivial Dirichlet character modulo $f$. Then

$$c_n(\chi) = \sum_{g \in \mathbb{M}_n} \Lambda(g)\chi(g) = \sum_{k|n} \sum_{P \in \mathbb{M}_{n/k}} \deg(P)\chi(P^k) = \sum_{k|n} \sum_{P \in \mathbb{M}_{n/k}} \deg(P)\chi(P)^k$$

$$= n \sum_{P \in \mathbb{M}_n} \chi(P) + \sum_{k \geq 2, P \in \mathbb{M}_n} \deg(P)\chi(P)^k,$$

where the last sum runs over all integers $k \geq 2$, and over all irreducible polynomials $P$ of $\mathbb{M}$ such that $k \deg(P) = n$. So,

$$\sum_{P \in \mathbb{M}_n} \chi(P) = \frac{1}{n} c_n(\chi) - \frac{1}{n} \sum_{k \geq 2, P \in \mathbb{M}_n} \deg(P)\chi(P)^k$$

and considering triangular inequalities

$$\left| \sum_{P \in \mathbb{M}_n} \chi(P) \right| \leq \frac{1}{n} |c_n(\chi)| - \frac{1}{n} \sum_{k \geq 2, P \in \mathbb{M}_n} \deg(P)\chi(P)^k.$$  \hspace{1cm} (2.11)

We have already bounded $|c_n|$ in Corollary 2.5.3, thus it remains to bound

$$\left| \sum_{k \geq 2, P \in \mathbb{M}_n} \deg(P)\chi(P)^k \right|.$$

We observe that

$$\sum_{k \geq 2, P \in \mathbb{M}_n} \deg(P)\chi(P)^k = \sum_{d|n} d \sum_{P \in \mathbb{M}_d} \chi(P)^{\frac{n}{d}}.$$  \hspace{1cm}

For the inner sum, by Theorem 2.3.4 we have

$$\left| \sum_{P \in \mathbb{M}_d} \chi(P)^{\frac{n}{d}} \right| \leq \sum_{P \in \mathbb{M}_d} |\chi(P)|^{\frac{n}{d}} \leq \sum_{P \in \mathbb{M}_d} 1 = I_d \leq \frac{q^d}{d} - \frac{q}{d}.$$
Hence, using again Theorem 2.3.4, we have

\[
\left| \sum_{k \geq 2, P \atop k \deg(P) = n} \deg(P) \chi(P)^k \right| = \left| \sum_{d \mid n \atop d \leq n/2} d \sum_{P \in I_d} \chi(P)^{\frac{n}{d}} \right| \leq \sum_{d \mid n \atop d \leq n/2} d \left( \sum_{P \in I_d} \chi(P)^{\frac{n}{d}} \right) \leq \sum_{d \mid n \atop d \leq n/2} d \left( q^{d} - \frac{q}{d} \right) \leq \sum_{d \mid n \atop d \leq n/2} q^{d} \leq \frac{q^{\lfloor n/2 \rfloor} - 1}{q - 1} \leq \frac{q^{\frac{n}{2}} - 1}{q - 1} \leq q^{\frac{n}{2}}.
\]

In conclusion

\[
\left| \sum_{k \geq 2, P \atop k \deg(P) = n} \deg(P) \chi(P)^k \right| \leq q^{\frac{n}{2}}. \tag{2.12}
\]

Hence, from (2.11), Corollary 2.5.3 and (2.12) we get

\[
\left| \sum_{P \in \mathfrak{I}_n} \chi(P) \right| \leq \frac{\deg(f) - 1}{n} q^{\frac{n}{2}} + \frac{q^{\frac{n}{2}}}{n} = \frac{\deg(f) - 1}{n} q^{\frac{n}{2}}.
\]

Remark 2.5.5. Weil’s Bound (Corollary 2.5.3), and the bound for $c'_n$ (Lemma 2.5.4) play a crucial role in the previous and new results to be presented in the following two chapters.
Chapter 3

Previous results on irreducible polynomials with prescribed coefficients

In this chapter we present the most important results regarding irreducible polynomials with prescribed coefficients. These results rely heavily on Weil’s bound (Corollary 2.5.3). Further improvements of this bound will result to analogous improvements of the results of this section. However, serious improvements would be a major achievement in this particular area of mathematics.

3.1 Generalizations of Dirichlet’s Theorem in \( F_q[x] \) and irreducible polynomials with prescribed coefficients

One of the most famous results in number theory was proved by Dirichlet in 1837 and it concerns the existence of prime numbers in arithmetic progressions.

**Dirichlet’s Theorem.** Let \( a \) and \( b \) be coprime positive integers. There are infinitely many prime numbers congruent to \( a \) modulo \( b \).

This theorem has its analogue in the ring of polynomials over finite fields.

**Dirichlet’s Theorem in \( A \).** Let \( f \) and \( g \) be coprime polynomials in \( A \) with \( f \) of positive degree. There are infinitely many monic irreducible polynomials congruent to \( g \) modulo \( f \).

**Remark 3.1.1.** In other words, Dirichlet’s Theorem in \( A \) says that there are infinitely many monic irreducible polynomials in arithmetic progressions of the form \( g + hf \), \( h \in A \), where \( f, g \) are coprime polynomials of \( A \) with \( f \) of positive degree.
All the results presented in this section are consequences of generalizations of Dirichlet’s Theorem in \( \mathbb{A} \). These generalizations yield not only the existence of infinitely many irreducible polynomials in arithmetic progressions, but they also give bounds for their number (related to their degrees).

Let \( \pi(n; f, g) \) be the number of polynomials of \( \mathbb{I}_n \) which are congruent to \( g \) modulo \( f \). Results concerning irreducible polynomials with prescribed coefficients are yielded by choosing suitable \( f \) and \( g \) so that \( \pi(n; f, g) \) expresses the number of such irreducible polynomials. More specifically, we have the following remark.

**Remark 3.1.2.** Let \( m, n \) be integers such that \( m \leq n \), \( f(x) = x^m \), and \( \alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_q \). Let \( g(x) = \alpha_{m-1}x^{m-1} + \cdots + \alpha_1 x + \alpha_0 \). Then \( \pi(n; f, g) \) is the number of polynomials in \( \mathbb{I}_n \) with their \( m \) least significant coefficients being \( \alpha_0, \ldots, \alpha_{m-1} \).

A classic result due to Artin [3] gives an approximation of \( \pi(n; f, g) \) when \( q \) is a prime number.

**Theorem (Artin).** Let \( p \) be a prime and \( f, g \in \mathbb{F}_p[x] \) such that \( (f, g) = 1 \). Then

\[
\pi(n; f, g) = \frac{p^n}{n\Phi(f)} + O\left(\frac{p^n}{n}\right),
\]

where \( \theta \) is a constant \(< 1 \).

We note that Dirichlet’s Theorem in \( \mathbb{F}_p[x] \) follows as an immediate consequence of Artin’s Theorem. This can be generalized for \( q \) being any prime power and with more specific bounds (also generalizing Dirichlet’s Theorem in \( \mathbb{A} \)). For instance, in [42, Theorem 5.1] we find the following theorem.

**Theorem 3.1.3.** Let \( f, g \in \mathbb{A} \) such that \( (f, g) = 1 \). Then

\[
\left| \pi(n; f, g) - \frac{q^n}{n\Phi(f)} \right| \leq \frac{1}{n}(\deg(f) + 1)q^{\frac{n}{2}}. \tag{3.1}
\]

Due to its importance and since it is a very good demonstration of how Weil’s bound can be used to obtain such results, we present here a more detailed version of the proof of Theorem 3.1.3.

**Proof of Theorem 3.1.3.** From part 2 of Proposition 2.4.6, we have that

\[
\frac{1}{\Phi(f)} \sum_{\chi \in X_f} \chi(P) \overline{\chi(g)} = \begin{cases} 1 & \text{if } P \equiv g \, (\text{mod } f); \\ 0 & \text{otherwise}. \end{cases}
\]
Thus, we have
\[
\pi(n; f, g) = \sum_{P \in I_n} \left( \frac{1}{\Phi(f)} \sum_{\chi \in X_f} \chi(P) \overline{\chi(g)} \right) = \frac{1}{\Phi(f)} \sum_{P \in I_n} \sum_{\chi \in X_f} \chi(P) \overline{\chi(g)} = \frac{1}{\Phi(f)} \sum_{\chi \in X_f} \sum_{P \in I_n} \chi(P) \overline{\chi(g)}.
\]

Subtracting \( q^n / (n\Phi(f)) \) from both sides of the equation above, taking absolute values and applying triangular inequalities, we have
\[
\left| \pi(n; f, g) - \frac{q^n}{\Phi(f)n} \right| \leq \frac{1}{\Phi(f)} \left( I_n - \frac{q^n}{n} \right) + \sum_{\chi \in X_f} \sum_{\chi \neq \chi_0} \left| \chi(g) \right| \left| \sum_{P \in I_n} \chi(P) \right|.
\]

From Theorem 2.3.4 and Lemma 2.5.4 we have
\[
\left| \pi(n; f, g) - \frac{q^n}{\Phi(f)n} \right| \leq \frac{1}{\Phi(f)} \left( I_n - \frac{q^n}{n} \right) + \sum_{\chi \in X_f} \sum_{\chi \neq \chi_0} \left| \chi(g) \right| \left| \sum_{P \in I_n} \chi(P) \right|.
\]

where the last equality comes from Corollary 2.4.5.

One of the most important results regarding irreducible polynomials of prescribed coefficients is a straightforward application of Theorem 3.1.3.

**Corollary 3.1.4.** Let \( m, n \) be positive integers and \( \alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_q \). There exists a polynomial in \( I_n \) with its \( m \) least significant coefficients being \( \alpha_0, \ldots, \alpha_{m-1} \), subject to \( m \leq n/2 - \log_q n \).
CHAPTER 3. PREVIOUS RESULTS

Proof. By Remark 3.1.2, the corollary can be proven by setting \( f(x) = x^m \), \( g(x) = \alpha_0 + \alpha_1 + \ldots + \alpha_{m-1}x^{m-1} \), and checking when the lower bound in (3.1) is strictly positive. So, by Proposition 2.1.12, in our case we need to have

\[
\frac{q^n}{nq^{m-1}(q-1)} - \frac{(m + 1)}{n} q^\frac{n}{2} > 0.
\]

We check that this holds when \( m \leq \frac{n}{2} - \log_q n \).

Remark 3.1.5. The bound for \( m \) in Corollary 3.1.12 can be slightly improved. However, this would make the derivation of the results that depend on it more complicated, without improving them significantly.

Corollary 3.1.4 shows that we can prescribe roughly half of the least significant coefficients of an irreducible polynomial. Using Lemma 2.1.16 we have that we can also prescribe roughly half of the most significant coefficients.

Corollary 3.1.6. Let \( m, n \) be positive integers and \( \alpha_1, \ldots, \alpha_{m-1} \in \mathbb{F}_q \). There exists a polynomial in \( \mathbb{F}_q \) with its \( m \) leading coefficients being \( 1, \alpha_1, \ldots, \alpha_{m-1} \), subject to \( m \leq n/2 - \log_q n \).

Proof. The proof is immediate from Corollary 3.1.4 with \( \alpha_0 = 1 \), and Lemma 2.1.16.

The above-mentioned results deal with irreducible polynomials with a number of either the least or most significant coefficients prescribed to any element. Further generalizations of Dirichlet’s Theorem in \( \mathbb{A} \) give results about the number of irreducible polynomials with least and most significant coefficients prescribed. Hayes [26] is the first to give such a result.
3.1. DIRICHLET’S THEOREM

Theorem (Hayes). Let \( k, n \) with \( 1 \leq k \leq n \), \( a = (\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_q^k \), and \( f, g \in \mathbb{A} \) such that \((f, g) = 1\). Denote by \( \pi(n; a, f, g) \) the number of polynomials \( P \in \mathbb{I}_n \) such that \( P \equiv g \pmod{f} \) and \( \deg(P - x^n - \alpha_1 x^{n-1} - \cdots - \alpha_k x^{n-k}) < n - k \). Then

\[
\pi(n; a, f, g) = \frac{q^{n-k}}{n \Phi(f)} + O\left(\frac{q^n}{n}\right),
\]

where \( \theta \) is a constant < 1.

We observe that Hayes’ theorem with \( f(x) = x^m \) and \( \deg(g) = m - 1 \) gives an approximation of the number of monic irreducible polynomials with the \( m \) least significant and \( k \) most significant coefficients prescribed to any elements.

Let \( \pi(n; k, f, g) \) denote the number of \( P \in \mathbb{I}_n \) such that \( P \equiv g \pmod{f} \) and

\[
\deg(P x^{\deg(g)} - g x^n) < n + \deg(g) - k.
\]

Remark 3.1.7. Let \( k, m, n \) be a positive integers and \( \alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_m \in \mathbb{F}_q \). Let \( f(x) = x^m \) and choose a \( g(x) \) of degree \( n + k + 1 \) with its \( k + 1 \) most significant coefficients being \( 1, \alpha_1, \ldots, \alpha_k \) and its \( m \) least significant coefficients being \( \beta_1, \ldots, \beta_m \). Then \( \pi(n; k, f, g) \) is the number of polynomials in \( \mathbb{I}_n \) with their \( k + 1 \) most significant coefficients being \( 1, \alpha_1, \ldots, \alpha_k \) and their \( m \) least significant coefficients being \( \beta_1, \ldots, \beta_m \).

Rhin [39] improves Hayes’ result in the following way.

Theorem 3.1.8. Let \( k, n \) be integers with \( 1 \leq k \leq n \) and \( f, g \in \mathbb{A} \). If \( k + \deg(g) \geq 1 \), we have

\[
\left| \pi(n; k, f, g) - \frac{q^{n-k}}{n \Phi(f)} \right| \leq (k + 1 + \deg(f))q^k.
\]

Hsu [27] further improves Hayes’s result with the following bounds.

Theorem 3.1.9. Considering the notations and conditions as in Theorem 3.1.8, we have

\[
\pi(n; k, f, g) \leq \frac{q^{n-k}}{n \Phi(f)} + \left(1 - \frac{1}{q^k \Phi(f)}\right) (k - 1 + \deg(f)) \frac{q^n}{n},
\]

\[
\pi(n; k, f, g) \geq \frac{q^{n-k}}{n \Phi(f)} - \left(1 - \frac{1}{q^k \Phi(f)}\right) (k + 3 + \deg(f)) \frac{q^n}{n} - \frac{\deg(f)}{n q^k \Phi(f)}.
\]
Further, Car [6] gives generalizations of results found in [27], also slightly improving the lower bound of Theorem 3.1.9.

**Corollary 3.1.10.** Again, with the notations and definitions as in Theorem 3.1.8, we have

\[
\pi(n; k, f, g) \geq \frac{q^{n-k}}{n\Phi(f)} - \left(1 - \frac{1}{q^k\Phi(f)}\right)(k - 1 + \deg(f)) \frac{q^n}{n} - \frac{2q^n}{n} - \frac{\deg(f)}{n}.
\]

Let \(a = (\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_q^k\) and \(b = (b_1, \ldots, b_m) \in \mathbb{F}_q^m\), and denote by \(\pi(n; a, b)\) the number of polynomials in \(I_n\) with their most significant coefficients being \(1, \alpha_1, \ldots, \alpha_k\) and their least significant coefficients being \(\beta_1, \ldots, \beta_m\). As we mentioned in Remark 3.1.7, \(\pi(n; a, b) = \pi(n; k, f, g)\) for \(f(x) = x^m\) and suitable choice of \(g\). Then, using Proposition 2.1.12, one derives from the above results bounds for \(\pi(n; a, b)\).

**Corollary 3.1.11.** Considering the above-mentioned notations, we have

\[
\pi(n; a, b) \leq \frac{q^{n-k-m+1}}{n(q-1)} + \left(1 - \frac{1}{q^{k+m-1}(q-1)}\right)(k + m - 1) \frac{q^n}{n},
\]

\[
\pi(n; a, b) \geq \frac{q^{n-k-m+1}}{n(q-1)} - \left(1 - \frac{1}{q^{k+m-1}(q-1)}\right)(k + m - 1) \frac{q^n}{n} - \frac{2q^n}{n} - \frac{m}{n}.
\]

To examine the existence of irreducible polynomials with the most and least significant coefficients prescribed, one has to check when the lower bound for \(\pi(n; a, b)\) is strictly positive.

**Corollary 3.1.12.** Let \(k, m, n\) be positive integers with \(1 \leq k, m \leq n\) and \(\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_m \in \mathbb{F}_q\). Then there exists a polynomial in \(I_n\) with its \(k + 1\) most significant coefficients being \(1, \alpha_1, \ldots, \alpha_k\) and its \(m\) least significant coefficients being \(\beta_1, \ldots, \beta_m\) subject to \(k + m \leq \frac{n}{2} - \log_q n\).

**Proof.** The proof is immediate, by checking that the lower bound in Corollary 3.1.11 is strictly positive when \(k + m \leq \frac{n}{2} - \log_q n\). \(\square\)

Figure 3.3: The graphical representation of Corollary 3.1.12.
### 3.2 The Hansen-Mullen Conjecture on irreducible polynomials with a prescribed coefficient

Hansen and Mullen [25] Conjecture that given integers $m, n$ with $n > m \geq 0$, there exists a polynomial in $\mathbb{F}_q$ with the coefficient of $x^m$ being any given element $\alpha \in \mathbb{F}_q$, where of course $\alpha \neq 0$ if $m = 0$. We observe that Corollaries 3.1.4 and 3.1.6 do not settle the conjecture when $|m - n/2| < \log_q n$. Using an estimate of a weighted sum, Wan [42, Corollary 5.3] shows the following.

**Corollary 3.2.1 (Wan).** Let $\alpha \in \mathbb{F}_q^*$ and $m, n$ positive integers with $n \geq 3$ and $m \leq n$. If

$$q^{n-m+1} \geq (q - 1)^2m^4,$$

then there exists a polynomial in $\mathbb{F}_q$ such that the coefficient of $x^{m-1}$ is $\alpha$.

Wan checks that (3.2) holds when $q > 19$ or $m \geq 36$, settling the conjecture for all but a finite number of cases, and the prescribed coefficient being nonzero. He explains however how one can settle the conjecture for the case when the prescribed coefficient is zero by a slight modification of his proof. Furthermore, by machine assisted computations, Ham and Mullen [24] verify the conjecture for the cases $q \leq 19$ and $m \leq 35$.

In Corollary 4.2.1, we give a generalization of Wan’s result (of which [42, Corollary 5.3] follows as a simple case) by giving conditions under which the Hansen-Mullen Conjecture can be extended to more than one prescribed coefficient. Moreover, considering Wan’s suggestion, this generalization also covers the case when the prescribed coefficient is zero.

We note that, unlike Corollaries 3.1.4, 3.1.6, and 3.1.12, Wan’s result on the existence of irreducible polynomials of a prescribed coefficient does not follow from an approximation of their number.

### 3.3 Irreducible polynomials with consecutive zero coefficients

Applications such as the *Coppersmith's Algorithm* [14] for efficient discrete logarithms computations, make use of irreducible polynomials with a large number of consecutive zero coefficients. It is thus natural to question the existence of irreducible polynomials of this particular form.

From Corollaries 3.1.4 and 3.1.6, the existence of polynomials in $\mathbb{F}_q$ with up to $n/2 - \log_q n$ of their most or least significant coefficients being zero (except of course the leading and the last), follows as an immediate consequence. Similarly, from Corollary 3.1.12 follows the existence of polynomials in
In with the \( m \) least and \( k \) most significant (apart from the leading) coefficients being zero, subject to \( k + m \leq n/2 - \log_q n \).

Garefalakis [21] proves that, asymptotically, there exist monic irreducible polynomials of degree \( n \) over \( \mathbb{F}_q \) with roughly \( n/3 \) consecutive coefficients being zero (not necessarily being the least or most significant ones). In particular, using techniques very similar to the ones Wan uses in his proof of [42, Corollary 5.3], he shows the following corollary.

**Corollary 3.3.1.** Let \( m, l, n \) be integers such that \( n > m > l > 1 \) and \( q^{n+l-2m} \geq qm^4 \). Then there exists a monic irreducible polynomial \( P(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathbb{F}_q \) such that \( a_{m-1} = \cdots = a_l = 0 \).

From Corollary 3.3.1, Garefalakis derives the following.

**Corollary 3.3.2.** Let \( 0 < c < 1 \) and \( n \) a positive integer such that \( (1 - 3c)n \geq 2 + 8 \log_q n \). Then there exists a monic irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \) with any \( \lfloor cn \rfloor \) consecutive coefficients, other than the first and the last, fixed to zero.

Corollary 3.3.2 shows that for any \( \varepsilon > 0 \) there exist monic irreducible polynomials of degree \( n \) with up to \( \lfloor (1/3 - \varepsilon)n \rfloor \) consecutive coefficients being zero, provided that \( n \) is large enough.

We note that the case of Corollary 3.3.1 where \( l = m - 1 \), settles the Hansen-Mullen Conjecture with the prescribed coefficient being zero, for all but a finite number of cases. In fact, Garefalakis starts from Wan’s suggestion for the proof of the zero case and extends it furthermore to yield his result.

Corollary 4.3.2 is a generalization of Corollary 3.3.1; conditions are given under which irreducible polynomials exist having more than one sequence of consecutive coefficients being zero.

### 3.4 Other results

The results presented so far are based on Weil’s Bound for character sums. For completeness, we briefly present in this section other results on irreducible polynomials with prescribed coefficients which are
3.4. OTHER RESULTS

3.4.1 Irreducible polynomials with a few non-zero coefficients

Definition 3.4.1. A binomial (trinomial, tetranomial, pentanomial) in $A$ is a polynomial with exactly 2 (3, 4, 5, respectively) non-zero coefficients.

We note that polynomials with a given number of non-zero terms are a special case of polynomials with prescribed coefficients. In general, it is unknown when a polynomial with a given number of non-zero coefficients is irreducible. Therefore, results characterizing the irreducibility of such polynomials are important and in the scope of this chapter.

In [32], one finds a necessary and sufficient condition related to $q$ for a binomial of $F_q[x]$ to be irreducible. In [37], Panario and Thomson, fixing a general $q$, determine for which $n$ there exist binomials in $I_n$.

Regarding trinomials in $F_2[x]$, Swan [41] gives criteria that decide about the parity of the number of their irreducible factors. He gives sufficient conditions for certain classes of trinomials to have an even number of irreducible factors, which yield a negative answer to the question of the existence of irreducible trinomials in such classes. For example, the following corollary follows from Swan’s results.

Corollary 3.4.2. If $8|n$ then there is no trinomial in $I_n$.

Swan’s results have recently been used by Brent and Zimmermann [5] to reduce the number of cases in a search for primitive trinomials over $F_2$ of very large degree. Moreover, there is active research for irreducibility criteria in $F_2[x]$ similar to the ones of Swan. Hales and Newhart [23] give a result similar to Swan for irreducible tetranomials in $F_2[x]$. Bluher [4] gives a Swan-like theorem for polynomials in $F_2[x]$ of the form $x^n + \sum_{i \in S} x^i + 1$, where $S \subset \{i; i \text{ odd, } 0 < i < n/3\} \cup \{i; i \equiv n \pmod{4}, 0 < i < n\}$.

Kim and Koepf [28] give a Swan-like result for the so-called type II binary pentanomials.

Regarding finite fields of odd characteristic, von zur Gathen [22] gives a table with conditions under which trinomials over $F_3$ are square-free and have an odd number of irreducible factors. Furthermore, he poses some conjectures on the distribution of irreducible trinomials over $F_3$, one of which is proven by Ahmadi [1]. Loidreau [33] gives the parity of the number of irreducible factors for any trinomial over $F_3$.

Regarding trinomials over general finite fields, using methods other than the ones of Swan, it has been proven independently by Cohen [9] and Ree [38] that given an integer $n > 1$, for large enough
There always exists an irreducible polynomial over $\mathbb{F}_q$ of the form $x^n + x + a$. However, no result follows from these works when $q$ is fixed and $n$ is large, or for the generic trinomial $x^n + ax^k + b$.

### 3.4.2 Irreducible polynomials with a few prescribed coefficients

Considering irreducible polynomials with a few coefficients prescribed, Corollaries 3.1.12 and 3.2.1, as well as some of our results of the next chapter yield existence results. However, there is also active research on the evaluation of their number. More precisely, there are studies on the number or irreducible polynomials of up to 3 most and/or least significant coefficients prescribed.

Carlitz [7] gives the number of irreducible polynomials with the first and last coefficients prescribed. Kuz’min [30, 31] does the same with the two most significant coefficients prescribed. Cattell et al. [8] also consider irreducible polynomials over $\mathbb{F}_2$ with the two most significant coefficients prescribed, using combinatorial techniques. Mullen and Yucas [35] and Fitzgerald and Yucas [20] consider irreducible polynomials over $\mathbb{F}_2$ with the 3 most significant coefficients prescribed. Kononen et al. [29], Moisio [34], and Omidi Koma et al. [36] consider irreducible polynomials with their trace and constant coefficient prescribed.
Chapter 4

New results on irreducible polynomials with prescribed coefficients

In this chapter we present the most significant part of our work. We prove our main theorem in the first section and we use it in the next ones to obtain some new results regarding irreducible polynomials with prescribed coefficients of several forms.

4.1 The main theorem

We use estimates of a product of weighted sums similar to the ones Wan uses in [42, Corollary 5.3], and Garefalakis [21] to obtain some new results regarding the existence of monic irreducible polynomials with prescribed coefficients. These follow from the next theorem.

Theorem 4.1.1. Let \( n \geq 3, m_1, \ldots, m_r, l_1, \ldots, l_r \) be integers such that \( n \geq m_1 \geq l_1 > m_2 \geq l_2 \cdots > m_r \geq l_r \geq 1 \) and \( \alpha_1, \ldots, \alpha_r \in \mathbb{F}_q^* \) with \( a_r \neq 0 \) if \( l_r = 1 \). Set \( m = \sum_{i=1}^{r} m_i \) and \( l = \sum_{i=1}^{r} l_i \). If

\[
n - 2(r + 1) \log_q n - 2 \log_q r - r \geq 2m - l,
\]

then there exists an irreducible polynomial of the form

\[
x^n + \sum_{i=0}^{n-1} a_i x^i, \quad a_i \in \mathbb{F}_q
\]

such that \( a_j = 0 \) for all \( m_i > j \geq l_i, 1 \leq i \leq r \), and \( a_j = \alpha_j \) for \( j = l_1 - 1, \ldots, l_r - 1 \).
Chapter 4. New Results

Proof of Theorem 4.1.1. Consider the product

\[ W = \sum_{h_1 \in \alpha_1 \mathbb{H}_{l_1-1}} \Lambda(h_1) \sum_{h_2 \in \alpha_2 \mathbb{H}_{l_2-1}} \Lambda(h_2) \cdots \sum_{h_r \in \alpha_r \mathbb{H}_{l_r-1}} \Lambda(h_r) \sum_{P} 1 \]  

(4.2)

where \( \Lambda \) is the von Mangoldt function (see Definition 2.1.14), \( \mathbb{H}_{l_i-1} \) is defined in Section 2.1.2, and the last sum is taken over all \( P \in \mathbb{I}_n \) such that \( P \equiv h_i \, (\text{mod } x^{m_i}), \, 1 \leq i \leq r \). Note that such a \( P \) is of the desired form, and all sums of the form

\[ \sum_{h_i \in \alpha_i \mathbb{H}_{l_i-1}} \Lambda(h_i) \]

are non-negative. Thus \( W \) being positive implies the existence of polynomials of the desired form.

The reason we use sums of this particular form is that they result in simpler estimates.

From our discussion above, our goal now becomes to prove that when condition (4.1) holds, \( W \) is positive. By the second part of Corollary 2.4.6 we can write \( W \) in the following way:

\[ W = \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \prod_{i=1}^{r} \sum_{h_i \in \alpha_i \mathbb{H}_{l_i-1}} \Lambda(h_i) \sum_{P \in \mathbb{I}_n} \prod_{j=1}^{r} \frac{1}{\chi_j(P)} \sum_{\chi_j} \chi_j(P) \chi_j(h_j) \]

where the sums \( \sum_{\chi_j} \) extend over all Dirichlet characters \( \chi_j \) modulo \( x^{m_j} \). Then

\[ W = \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \prod_{i=1}^{r} \sum_{h_i \in \alpha_i \mathbb{H}_{l_i-1}} \Lambda(h_i) \sum_{P \in \mathbb{I}_n} \prod_{s=1}^{r} \sum_{\chi_s} \chi_s(P) \chi_s(h_s) \]

\[ = \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \prod_{i=1}^{r} \sum_{h_i \in \alpha_i \mathbb{H}_{l_i-1}} \Lambda(h_i) \sum_{P \in \mathbb{I}_n} \prod_{(\chi_1, \ldots, \chi_r) = 1}^{r} \sum_{s=1}^{r} \prod_{t=1}^{r} \chi_t(P) \chi_t(h_t) \]
where the sum $\sum_{(\chi_1, \ldots, \chi_r)}$ is extended over all the $r$-tuples $(\chi_1, \ldots, \chi_r) \in X_{x^{m_1}} \times \cdots \times X_{x^{m_r}}$. Then

$$W = \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{\chi_1, \ldots, \chi_r} \prod_{i=1}^{r} \sum_{\lambda_i, \lambda_{i-1}} \Lambda(h_i) \prod_{t=1}^{r} \chi_i(h_t) \sum_{P \in \mathbb{P}} \prod_{s=1}^{r} \chi_s(P)$$

$$= \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{\chi_1, \ldots, \chi_r} \prod_{i=1}^{r} \sum_{\lambda_i, \lambda_{i-1}} \Lambda(h_i) \chi_i(h_t) \sum_{P \in \mathbb{P}} \prod_{s=1}^{r} \chi_s(P)$$

$$= \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{\chi_1, \ldots, \chi_r} \prod_{i=1}^{r} \chi_i(h_t) \sum_{P \in \mathbb{P}} \prod_{s=1}^{r} \chi_s(P),$$

where $\chi_1, \ldots, \chi_r$ is the Dirichlet character modulo $x^{m_1} \cdots x^{m_r} = x^m$ that maps $P$ to $\prod_{i=1}^{r} \chi_i(P)$ (see Lemma 2.4.8). We observe that

$$\sum_{h_i \in \mathbb{H}_{i-1}} \Lambda(h_i) \chi_i(h_t) = \sum_{h_i \in \mathbb{H}_{i-1}} \Lambda(\alpha_i h_i) \chi_i(\alpha_i h_t) = \sum_{h_i \in \mathbb{H}_{i-1}} \Lambda(h_i) \chi_i(\alpha_i) \chi_i(h_t)$$

$$= \chi_i(\alpha_i) \sum_{h_i \in \mathbb{H}_{i-1}} \Lambda(h_i) \chi_i(h_t).$$

Then, considering $c_n$ and $c'_n$ as defined in Lemmas 2.5.1 and 2.5.4, respectively, we have

$$W = \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{\chi_1, \ldots, \chi_r} \prod_{i=1}^{r} \chi_i(\alpha_i) \sum_{h_i \in \mathbb{H}_{i-1}} \Lambda(h_i) \chi_i(h_t) \sum_{P \in \mathbb{P}} \prod_{s=1}^{r} \chi_s(P)$$

$$= \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{\chi_1, \ldots, \chi_r} \prod_{i=1}^{r} \chi_i(\alpha_i) c_{i-1}(\chi) c'_n \chi_1, \ldots, \chi_r).$$

Denote by $\chi_{i_0}$ the trivial Dirichlet character modulo $x^{m_1}$ and by $\chi_0$ the trivial Dirichlet character modulo $x^m$. Observing that $\overline{\chi_{i_0}} = \chi_{i_0}$, we have

$$W = \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \prod_{i=1}^{r} c_{i-1}(\chi_{i_0}) c'_n(\chi_0)$$

$$+ \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{\chi_1, \ldots, \chi_r \neq (\chi_{i_0}, \ldots, \chi_{i_0})} \prod_{i=1}^{r} \chi_i(\alpha_i) c_{i-1}(\chi_0) c'_n \chi_1, \ldots, \chi_r),$$

where the sum is extended over all the $r$-tuples $(\chi_1, \ldots, \chi_r) \in X_{x^{m_1}} \times \cdots \times X_{x^{m_r}}$ with $(\chi_1, \ldots, \chi_r) \neq (\chi_{i_0}, \ldots, \chi_{i_0})$.
\((\chi_{10}, \ldots , \chi_{r0})\). From Corollary 2.5.3 and Lemma 2.5.4 we have

\[
\prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \prod_{i=1}^{r} c_{l-1}(\chi_i)c'_n(\mathcal{X}_0) = I_n \frac{q^{l-m}}{(q-1)^r}.
\]

So

\[
W - I_n \frac{q^{l-m}}{(q-1)^r} = \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{(\chi_1, \ldots , \chi_r) \neq (\chi_{10}, \ldots , \chi_{r0})} \chi_i(\alpha_i) \prod_{i=1}^{r} c_{l-1}(\chi_i)c'_n(\mathcal{X}_1, \ldots , r).
\]

Taking absolute values, applying triangular inequalities, considering the fact that \(|\chi_i(\alpha_i)| = 1\) for all \(i \in \{1, \ldots , r\}\), and using the bounds given in Corollary 2.5.3 and Lemma 2.5.4, we get

\[
|W - I_n \frac{q^{l-m}}{(q-1)^r}| \leq \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{(\chi_1, \ldots , \chi_r) \neq (\chi_{10}, \ldots , \chi_{r0})} \prod_{i=1}^{r} c_{l-1}(\chi_i) |c'_n(\mathcal{X}_1, \ldots , r)|
\]

\[
\leq \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{(\chi_1, \ldots , \chi_r) \neq (\chi_{10}, \ldots , \chi_{r0})} \prod_{i=1}^{r} (m_i - 1) q^{i-1} \frac{m}{n} \frac{n}{q^n}
\]

\[
= q^{\frac{a+1-r}{n}} \prod_{j=1}^{r} \frac{1}{\Phi(x^{m_j})} \sum_{(\chi_1, \ldots , \chi_r) \neq (\chi_{10}, \ldots , \chi_{r0})} 1,
\]

(4.3)

where \(M = m \prod_{i=1}^{r} (m_i - 1)\). Now, by Corollary 2.4.5

\[
\sum_{(\chi_1, \ldots , \chi_r) \neq (\chi_{10}, \ldots , \chi_{r0})} 1 = \prod_{i=1}^{r} \Phi(x^{m_i}) - 1
\]

so

\[
\prod_{i=1}^{r} \frac{1}{\Phi(x^{m_i})} \sum_{(\chi_1, \ldots , \chi_r) \neq (\chi_{10}, \ldots , \chi_{r0})} 1 < 1
\]

and by (4.3) we conclude that

\[
|W - I_n \frac{q^{l-m}}{(q-1)^r}| < q^{\frac{a+1-r}{2}} \frac{M}{n}.
\]

Hence

\[
W > I_n \frac{q^{l-m}}{(q-1)^r} - q^{\frac{a+1-r}{2}} \frac{M}{n}
\]
and from Theorem 2.3.4 we have

\[ W > \left( \frac{q^n}{n} - 2q^{\frac{n}{2}} \right) \frac{q^{l-m}}{(q-1)^r} - q^{\frac{n+l-r}{2}} \frac{M}{n} \]

\[ = \frac{1}{n} \left( q^{n+l-m} - \frac{2q^{\frac{n+l-m}{2}} - (q-1)^r - Mq^{\frac{n+l-r}{2}}} {q^{\frac{n+l-m}{2}}} \right) \]

\[ > \frac{1}{n} \left( q^{n+l-m-r} - 2q^{\frac{n+l-m}{2}} - (M + 1)q^{\frac{n+l-r}{2}} + q^{\frac{n+l-r}{2}} \right) \]

\[ = \frac{1}{n} \left( q^{n+l-m-r} - (M + 1)q^{\frac{n+l-r}{2}} + \left( q^{\frac{n+l-r}{2}} - 2q^{\frac{n+l-m}{2}} \right) \right) \]

\[ \geq \frac{1}{n} \left( q^{n+l-m-r} - (M + 1)q^{\frac{n+l-r}{2}} \right) \]

\[ = \frac{q^{\frac{n+l-r}{2}}}{n} \left( q^{\frac{n+l-r}{2}} - m - (M + 1) \right) \]

where the last inequality is yielded by easily checking that

\[ q^{\frac{n+l-r}{2}} - 2q^{\frac{n+l-m}{2}} \frac{M}{(q-1)^r} > 0. \]

From the above, we have that a sufficient condition for \( W \) to be positive is

\[ q^{\frac{n+l-r}{2}} - m -(M + 1) \geq 0 \quad (4.4) \]

or

\[ n - r - 2 \log_q (M + 1) \geq 2m - l. \]

We easily check that \( M + 1 \leq rnr^{r+1}, \) so a sufficient condition for \( W \) to be positive is

\[ n - 2(r + 1) \log_q n - 2 \log_q r - r \geq 2m - l. \]

Subject to this, \( W \) is positive and hence polynomials of the desired form exist.

Remark 4.1.2. A very crucial step of the proof of Theorem 4.1.1 is (4.3), since the power of \( q \) that appears in (4.3) is directly connected to (4.1). It is thus clear that Weil’s bound (2.5.3) plays a very
important role in this proof. Moreover, this proof is heavily based on the proof of [42, Corollary 5.3] and, in fact, Weil’s bound is significant for this important result, in a very similar way.

Considering the case \( r = 1, m_1 = l_1 \) of Theorem 4.1.1 yields something very similar to Corollary 3.2.1 ([42, Corollary 5.3]).

**Corollary 4.1.3.** Let \( \alpha \in \mathbb{F}_q \) and \( m, n \) positive integers with \( n \geq 3 \) and \( m \leq n \). If

\[
q^{n-m+1} \geq q^2 n^4, \tag{4.5}
\]

then there exists a polynomial in \( \mathbb{I}_n \), such that the coefficient of \( x^{m-1} \) is \( \alpha \).

**Remark 4.1.4.** The \( n^4 \) on the right side of (4.5) could be replaced by \( m^4 \) if we had used (4.4) instead of (4.1), which we did not for simplicity. Furthermore, the reason that \( q^2 \) appears in (4.5) instead of \( (q-1)^2 \) as in (3.2), is that Corollary 3.2.1 does not cover the case \( \alpha = 0 \).

**Remark 4.1.5.** We have that [21, Corollary 2] follows as the case \( r = 1, \alpha = 1 \) of Theorem 4.1.1.

### 4.2 A generalization of the Hansen-Mullen Conjecture on irreducible polynomials with a prescribed coefficient

Theorem 4.1.1 gives conditions under which we can prescribe any coefficient of an irreducible polynomial to any value.

**Corollary 4.2.1.** Let \( n \geq 3, m_1, m_2, \ldots, m_r \) be integers such that \( n \geq m_1 > \cdots > m_r \geq 1 \) and \( \beta_1, \ldots, \beta_r \in \mathbb{F}_q \) with \( \beta_r \neq 0 \) if \( m_r = 1 \). If

\[
m_1 + m_2 + \cdots + m_r \leq n - 2(r+1) \log_q n - 2 \log_q r - 3r, \tag{4.6}
\]

then there exists a polynomial in \( \mathbb{I}_n \), such that the coefficient of \( x^{m_i-1} \) is \( \beta_i, i = 1, \ldots, r \)

**Proof.** Consider Theorem 4.1.1 with \( \beta_i = \alpha_i, m_i = l_i \) if \( \beta_i \neq 0 \), and \( l_i = m_i - 2 \) if \( \beta_i = 0 \). The value of \( \alpha_i \) in that latter case is insignificant, so we may as well ignore it. Since \( l_i \geq m_i - 2 \) for all \( i \), we have that \( l \geq m - 2r \) and thus \( m + 2r \geq 2m - l \). Thus, instead of (4.1) we may use the sufficient condition \( n - 2(r+1) \log_q n - 2 \log_q r - r \geq m + 2r \), which can be rewritten as \( m_1 + \cdots + m_r \leq n - 2(r+1) \log_q n - 2 \log_q r - 3r \). We observe that the irreducible polynomial whose existence is yielded in the case described above is of the desired form. \( \Box \)
Corollary 4.2.1 shows that we can prescribe any coefficients of an irreducible polynomial under the condition that the sum of the corresponding powers is roughly \( n \). This becomes quite restrictive when \( r \) is large, however small values of \( r \) give some interesting results.

As we mentioned earlier, it follows from [42, Corollary 5.3] and [24] that the Hansen-Mullen Conjecture is true, that is, given an element \( \alpha \) of \( \mathbb{F}_q \) and \( n \in \mathbb{N} \), there exists a polynomial in \( \mathbb{I}_n \) with any one of its coefficients being \( \alpha \). It is natural to ask if this can be generalized to more than one prescribed coefficients. Corollary 4.2.1 along with Corollary 3.1.12, gives an answer to this question.

**Corollary 4.2.2.** Let \( n \geq 3, m_1, \ldots, m_r \) be integers such that \( n \geq m_1 > \cdots > m_r \geq 1 \) and \( \alpha_1, \ldots, \alpha_r \in \mathbb{F}_q \), with \( \alpha_r \neq 0 \) if \( m_r = 1 \). If

\[
m_2 \leq \frac{n}{2r} - \frac{2r + 3}{r} \log_q n - \frac{2}{r} \log_q r - 3
\]

or

\[
m_{r-1} \geq \frac{2r - 1}{2r} n + \frac{2r + 3}{r} \log_q n + \frac{2}{r} \log_q r + 3,
\]

then there exists a polynomial in \( \mathbb{I}_n \) with the coefficient of \( x^{m_i - 1} \) being \( \alpha_i \), \( i = 1, \ldots, r \).

**Proof of Corollary 4.2.2.** When \( m_2 + (n - m_1 + 1) \leq n/2 - \log_q n \), or equivalently \( m_1 \geq n/2 + m_2 + \log_q n + 1 \), our corollary is a simple case of Corollary 3.1.12. We now consider the case \( m_1 \leq n/2 + m_2 + \log_q n \). Since \( m_1 + m_2 + \cdots + m_r \leq m_1 + (r - 1)m_2 \), from (4.6) the corollary is settled whenever

\[
m_1 \leq n - (r - 1)m_2 - 2(r + 1) \log_q n - 2 \log_q r - 3r,
\]

Figure 4.2: The graphical representation of Theorem 4.2.2.
so our corollary follows when

\[ \frac{n}{2} + m_2 + \log_q n \leq n - (r - 1)m_2 - 2(r + 1)\log_q n - 2\log_q r - 3r, \]

or equivalently,

\[ m_2 \leq \frac{n}{(2r)} - (2r + 3)(\log_q n)/r - (2\log_q r)/r - 3, \]

which proves the first case. The case

\[ m_{r-1} \geq (2r - 1)n/(2r) + (2r + 3)(\log_q n)/r + (2\log_q r)/r + 3 \]

is an immediate consequence of Lemma 2.1.16.

Corollary 4.2.2 shows that, for sufficiently large \( n \) or \( q \), we can prescribe \( r - 1 \) of the roughly \( n/(2r) \) most or least significant coefficients, and another arbitrary one, of a polynomial in \( \mathbb{I}_n \). We examine some interesting cases, in particular, when \( r = 2, 3 \).

**Corollary 4.2.3.** Let \( n, m_1, m_2 \) be integers such that \( n \geq m_1 > m_2 \geq 1 \) and \( \alpha_1, \alpha_2 \in \mathbb{F}_q \), with \( \alpha_2 \neq 0 \) if \( m_2 = 1 \). If

\[ m_2 \leq \frac{n}{4} - \frac{7}{2} \log_q n - \log_q 2 - 3 \]

or

\[ m_1 \geq \frac{3n}{4} + \frac{7}{2} \log_q n + \log_q 2 + 3, \]

then there exists a polynomial in \( \mathbb{I}_n \) such that the coefficients of \( x^{m_1-1}, x^{m_2-1} \) are \( \alpha_1 \) and \( \alpha_2 \) respectively.

Setting \( m_1 = n \) in the above corollary we have that, for sufficiently big \( n \) or \( q \), we can always prescribe the trace and any other coefficient of a polynomial in \( \mathbb{I}_n \) to any value.

**Corollary 4.2.4.** Let \( n \geq 14\log_q n + \log_q 16 + 12 \), and \( \alpha, \beta \in \mathbb{F}_q \). There exists a monic irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \) with trace \( \alpha \) and any other coefficient being \( \beta \) (with \( \beta \neq 0 \) for the constant coefficient).

For the case of three prescribed coefficients, Corollary 4.2.1 gives the following.
Corollary 4.2.5. Let \( n \geq 3, m_1, m_2, m_3 \) be integers such that \( n \geq m_1 > m_2 > m_3 \geq 1 \), and \( \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_q \), with \( \alpha_3 \neq 0 \) if \( m_3 = 1 \). If

\[
m_2 \leq \frac{n}{6} - 3\log_q n - \frac{2}{3}\log_q 3 - 3
\]

or

\[
m_2 \geq \frac{5n}{6} + 3\log_q n + \frac{2}{3}\log_q 3 + 3,
\]

then there exists a polynomial in \( \mathbb{F}_q \) such that the coefficients of \( x^{m_1-1}, x^{m_2-1}, x^{m_3-1} \) are \( \alpha_1, \alpha_2 \) and \( \alpha_3 \) respectively.

In that case, considering traces and subtraces with prescribed coefficients, the above corollary gives the following result.

Corollary 4.2.6. Let \( \alpha, \beta, \gamma \in \mathbb{F}_q \) and \( n \) be an integer such that \( n \geq 18 \log_q n + 4 \log_q 3 + 18 \). Then there exists a monic irreducible polynomial of degree \( n \) over \( \mathbb{F}_q \) with trace \( \alpha \), subtrace \( \beta \), and any other coefficient being \( \gamma \) (\( \gamma \neq 0 \) for the constant coefficient).

4.3 Irreducible polynomials with consecutive zero coefficients

In this section we use Theorem 4.1.1 to examine the existence of irreducible polynomials with prescribed coefficients of forms that cannot be obtained from the existing results presented so far.

We first start with a definition.

Definition 4.3.1. Let \( n, m, k \) be integers such that \( 0 \leq k < m \leq n \) and \( f(x) = \sum_{i=0}^{n} a_n x^n \). We call \( a_m, a_{m-1}, \ldots, a_{m-k+1} \) a sequence of coefficients of \( f \) of length \( k \) beginning from \( x^m \). The total length of two or more such sequences is the sum of their individual lengths.

More specifically, we examine the existence of irreducible polynomials with sequences of coefficients prescribed to zero. Focusing on that question, we present the following simpler version of Theorem 4.1.1.

Corollary 4.3.2. Let \( n \geq 3, m_1, \ldots, m_r, l_1, \ldots, l_r \) integers such that \( n \geq m_1 > l_1 \geq m_2 > l_2 \ldots m_r > l_r \geq 1 \). Set \( m = \sum_{i=1}^{r} m_i \), \( l = \sum_{i=1}^{r} l_i \). If

\[
n - 2(r + 1) \log_q n - 2 \log_q r - r \geq 2m - l,
\]
then there exists an irreducible polynomial of the form \( x^n + \sum_{i=0}^{n-1} a_i x^i \), \( a_i \in \mathbb{F}_q \) such that \( a_j = 0 \) for all \( m_i > j \geq l_i, 1 \leq i \leq r \).

Figure 4.3: The graphical representation of Theorem 4.3.2.

We present some examples of the above corollaries that cannot be obtained using the results of Chapter 3.

**Corollary 4.3.3.** Let \( \alpha \in \mathbb{F}_q \) and \( c \) be a real number such that \( 0 < c < 1/4 \). Then there exists an integer \( n \) and a polynomial in \( \mathbb{I}_n \) with trace \( \alpha \) and a sequence of \( \lfloor cn \rfloor \) consecutive zero coefficients.

![Diagram](image)

**Figure 4.4: The graphical representation of Corollary 4.3.3.**

**Proof of Corollary 4.3.3.** Considering Lemma 2.1.16, we can equivalently prove that there exists an integer \( n \) and a polynomial in \( \mathbb{I}_n \) with the coefficient of \( x \) being \( \alpha \) and a sequence of \( \lfloor cn \rfloor \) consecutive zero coefficients.

Let \( n \) be a positive integer, and consider Theorem 4.1.1 with \( r = 2, m_2 = l_2 = 2, \alpha_1 = \alpha \) and set \( m_1 - l_1 = \lfloor cn \rfloor \). When \( 2 + (n - l_1 + 1) \leq n/2 - \log_q n \), or equivalently \( l_1 \geq n/2 + \log_q n + 3 \), then our corollary follows from Corollary 3.1.12. Now, let

\[
l_1 \leq n/2 + \log_q n + 2.
\]

From (4.1), our Corollary follows whenever

\[
n - 6 \log_q n - 2 \log_q 2 - 2 \geq 2m - l.
\]
4.3. CONSECUTIVE ZERO COEFFICIENTS

We observe that \(2m - l \leq m + cn = m_1 + cn + 2\), hence a sufficient condition is given by

\[ n - 6 \log_q n - 2 \log_q 2 - 2 \geq m_1 + cn + 2, \]

or equivalently

\[ m_1 \leq n(1 - c) - 6 \log_q n - 2 \log_q 2 - 4. \]

Because \(m_1 \leq l_1 + cn\), we also have the sufficient condition

\[ l_1 + cn \leq n(1 - c) - 6 \log_q n - 2 \log_q 2 - 4, \]

or equivalently,

\[ l_1 \leq (1 - 2c)n - 6 \log_q n - 2 \log_q 2 - 4. \quad (4.8) \]

When (4.8) holds, then there exists an irreducible polynomial of the desired form. From (4.7) and (4.8), we have that the corollary follows whenever

\[ \frac{n}{2} + \log_q n + 2 \leq (1 - 2c)n - 6 \log_q n - 2 \log_q 2 - 4, \]

or equivalently,

\[ \left(\frac{1}{2} - 2c\right)n \geq 7 \log_q n + 2 \log_q 2 + 6. \quad (4.9) \]

Since \(0 < c < 1/4\), then \((1/2 - 2c) > 0\). We observe that \(n\) can be chosen sufficiently large so that (4.9) holds. That completes the proof of the corollary.

We now consider polynomials over \(\mathbb{F}_2\) of the form \(\sum_{i=0}^{\log_2 n} x^{2^i}\). We use Theorem 4.1.1 to obtain the existence of irreducible polynomials that are partially of this form.

Let \(k\), with \(n \geq k > 0\), be a power of 2, and let \(l_i = 2^{\log_2 k + 1 - i} + 1, m_i = 2^{\log_2 k + 2 - i} - 1, i = 1, 2, \ldots, \log_2 k\). For these choices of \(m_i\) and \(l_i\), and when (4.1) holds, Theorem 4.1.1 yields the existence of polynomials of the form as in Figure 4.5.

In our case, (4.1) becomes

\[ n - 2(\log_2 k + 1) \log_2 n - 2 \log_2 (\log_2 k) \geq 2m - l = 6k - 3 \log_2 k - 6. \quad (4.10) \]
Thus, another sufficient condition for polynomials as in figure 4.5 to exist, is

\[ k \leq \frac{n}{6} - \frac{1}{3} (\log_2 n)^2 + \frac{2}{3} \log_2 n. \]

**Example 4.3.4.** There exists an irreducible polynomial with degree \( n = 2^{11} \) over \( \mathbb{F}_2 \) of the form \( P(x) = 1 + \sum_{i=1}^{2^{11}-1} a_i x^i + x^{2^{11}} \) such that, for all \( i, 1 \leq i \leq 2^8 \), we have

\[ a_i = \begin{cases} 
1 & \text{when } i \text{ is a power of } 2, \\
0 & \text{otherwise.}
\end{cases} \]

This follows from the fact that (4.10) holds when \( n = 2^{11} \) and \( k = 2^8 \) (but not when \( k = 2^9 \)).
Chapter 5

Conclusions

5.1 Summary of results

In this thesis, we consider the existence of irreducible polynomials with prescribed coefficients. We present existing and new results that are based on number theoretical tools in the context of the ring of polynomials over finite fields, namely Dirichlet characters, and bounds of certain character sums.

We devote Chapter 3 to the existing results, focusing on two classes. The first one is presented in Section 3.1, and concerns the results that are obtained from variations of Dirichlet’s Theorem in the context of the ring of polynomials over finite fields. A detailed proof of a quantitative version of Dirichlet’s theorem is given. In the end of that section we present the following.

Result 1. If $k + m$ is roughly less than $n/2$, then we can prescribe the $k+1$ most and $m$ least significant coefficients of a polynomial in $\mathbb{I}_n$ (apart from the leading and constant one) to any element of $\mathbb{F}_q$ (see Figure 3.3).

The second class concerns the results that are obtained using variations of a certain character sum and are presented in Sections 3.2 and 3.3. From the discussion in Section 3.2 follows the proof of the Hansen-Mullen conjecture.

Result 2 (Wan). Let $n \geq 3$. We can prescribe any coefficient of a polynomial in $\mathbb{I}_n$ to any element of $\mathbb{F}_q$.

From the discussion in Section 3.3, we have the following.

Result 3 (Garefalakis). For sufficiently large $n$, there exists a polynomial in $\mathbb{I}_n$ with roughly $n/3$ consecutive zero coefficients (see Figure 3.4).
In Chapter 4 we present our main theorem, that we use to obtain various results. One of them gives a weak generalization of the Hansen-Mullen Conjecture to more than one prescribed coefficients.

**Result 4.** There exists a polynomial in $I_n$ with $r$ coefficients prescribed to any element of $\mathbb{F}_q$, if at least $r - 1$ of them are among the $n/2r$ most or least significant ones (see Figure 4.2).

We also give some interesting consequences of the above results when $r = 2$ or 3.

In Section 4.3 we use our main Theorem to obtain results regarding irreducible polynomials with sequences of zero coefficients. In the end of the section, we show the following.

**Result 5.** For sufficiently large $n$, there exists a polynomial in $I_n$ with its trace prescribed to any element of $\mathbb{F}_q$ and a sequence of roughly $n/4$ consecutive zero coefficients (see Figure 4.4).

### 5.2 Open questions for further work

Our discussion on irreducible polynomials with prescribed coefficients leads to some related questions of the same nature.

**Question 1.** Theorem 4.1.1, which is the main result of our work, has a quite restrictive condition, namely, (4.1) must hold for the polynomials of our interest to exist. Can this condition be relaxed? If so, all the following results of Chapter 4 will consequently be improved.

We note that (4.1) heavily relies on Weil’s Bound (Corollary 2.5.3). If there is an improvement of this bound, then the results of Chapter 4 will be improved accordingly. However, improving Weil’s bound is considered to be a very difficult problem.

**Question 2.** All our new results concern the existence of irreducible polynomials of certain forms. Can one also give an estimate for the number of such polynomials?

A natural way to attempt to find such estimates, would be to change $W$ in 4.2 so that it expresses the exact number of the desired polynomials. However, this does not seem to be straightforward if we try to use similar ideas to the ones in the proof of Theorem 4.1.1 for this ‘new’ $W$. For instance, consider a fixed $\alpha \in \mathbb{F}_q$ and

$$W' = \sum_{h \in \alpha M_{l-1}} \sum_{\substack{P \in I_n \equiv h \pmod{x^m}}} 1.$$  

We observe that $W'$ gives the number of irreducible polynomials of the form described in Theorem 4.1.1 for $r = 1$. If we reproduce the steps of the proof of the theorem, this time to give an estimate
for \( W' \), we need at some point a non-trivial bound for a sum of the form \( |\sum_{h \in M_l} \chi(h)| \), where \( \chi \) is a Dirichlet character modulo \( x^m \). Such bounds have not been proven to our knowledge. If such a bound is given, then we can have quantitative versions of the existence results of Chapter 4.

Question 3. Can the Hansen-Mullen conjecture be settled for more than one coefficients? In other words, can (4.6) be removed or replaced by a condition that holds for large enough \( n \)?

Although experimental results suggest that one may prescribe roughly \( n - \log_q n \) of the coefficients of a polynomial in \( \mathbb{I}_n \), the proof of this would be a major result of this particular area of mathematics. It would be more reasonable to attempt to answer Question 3 for \( r = 2 \). Moreover, our generalization of Wan’s proof of the Hansen-Mullen conjecture, could not fully settle Question 3, although it seems to be the most natural one; we believe that, to attempt this, one should use different methods.
Bibliography


